A FAMILY OF UNSPLITTABLE MINIMAL ZERO-SUM SEQUENCES

Fang Chen
Oxford College of Emory University, Oxford, Georgia
fchen2@emory.edu

Received: 7/27/21, Accepted: 1/21/22, Published: 2/7/22

Abstract

A minimal zero-sum sequence α over a finite abelian group G is unsplittable if replacing any term t of α by any two elements of G with sum t yields a zero-sum sequence that is not minimal. This article characterizes a family of unsplittable minimal zero-sum sequences that includes most of the nontrivial ones known so far.

1. Introduction

A nonempty sequence over an additively written finite abelian group is a *minimal zero-sum sequence* if its sum is the zero element of the group and all of its proper nonempty subsequences have nonzero sums. Gao [1] introduced the notion of an *unsplittable sequence* (Definition 1), which is a minimal zero-sum sequence such that no term can be replaced by two group elements without violating the minimality. These are minimal zero-sum sequences extremal in a well-defined sense; they enjoy certain properties of the longest minimal zero-sum sequences (Lemmas 1 and 2). Unsplittable sequences are more convenient to work with, and knowledge about them often imply results on general minimal zero-sum sequences. Consequently, they have been studied with much interest, especially in finite cyclic groups with connection to the index and related problems [1, 2, 3, 5, 6, 7, 8, 9].

In [4], an approach with a strong emphasis on unsplittable sequences was chosen in order to characterize the minimal zero-sum sequences over the cyclic group C_n with lengths at least $\lfloor n/3 \rfloor + 3$. The results indicate that not only the unsplittable sequences are more flexible to work with, but also that the notion itself deserves attention and understanding in its own right. In particular, it obtained the following explicit description of the unsplittable minimal zero-sum sequences over C_n with lengths in $[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1]$, for all $n \geq 10$.

Theorem 1 ([4], Theorem 7.8). *A sequence over the cyclic group C_n, $n \geq 10$, with length in the range $[\lfloor n/3 \rfloor + 3, \lfloor n/2 \rfloor + 1]$ 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) $u \neq 0$, $v \notin \{u, 2u, \ldots, (p+1)u\}$, $1 \leq s \leq p < \mathrm{ord}(u)$, *and* $q \geq 1$*;*

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

It was pointed out that the length condition is only needed in the necessity part. In other words, a sequence of the form $u^p v^q(v - su)$ that satisfies conditions (i)–(iv) of Theorem 1 is an unsplittable minimal zero-sum sequence.

In this article, we drop the length condition and study sequences of a form generalizing the ones in Theorem 1, called *admissible* (Definition 2). We will characterize when such sequences are unsplittable. It is worth noting that so far most of the unsplittable sequences appeared in applications are admissible. The main theorem (Theorem 2) reveals that this family has a nice structure with pleasant properties. Our approach is completely combinatorial. We hope that the techniques developed will be useful in the investigation of other unsplittable sequences.

Here is the organization of the article. Section 2 begins with preparatory definitions and terminology. We also recall some basic properties of unsplittable sequences and state the main result (Theorem 2). The core of the work is in Section 3, which contains several key lemmas about the sequences being studied. The proof of Theorem 2 is presented in Sections 4 and 5.

2. Preliminaries

Henceforth G denotes an additively written finite abelian group, and $G^\bullet = G \setminus \{0\}$.

As this paper extends a situation in [4], we adopt some notation and terminology from that article. A *sequence* means a *finite multiset* throughout the text. So, informally speaking, a sequence over G is a finite unordered collection of group elements with repetitions allowed. These elements are called *terms* of the sequence. For a sequence α over G and $a \in G$, the notation $a \in \alpha$ means that a is a term of α. The *multiplicity* in α of a term $a \in \alpha$ is the number of times a occurs in α, and we denote it by m_a (α is always clear from the context). The order of an element $a \in G$ is denoted by $\mathrm{ord}(a)$.

Our sequence notation is multiplicative: if α is a sequence with terms $a_1, \ldots, a_k$ we write $\alpha = a_1 \cdots a_k$. Whenever necessary, term multiplicities are indicated by exponents; for example $\alpha = u^p v^q$ denotes the sequence α with p terms equal to u

and q terms equal to v. For a subsequence β of α we write $\beta|\alpha$. However, since sequences are viewed as multisets, we prefer the notation $a \in \alpha$ for the one-term subsequence $\beta = a$ of α. The complementary subsequence of β is denoted by $\alpha\beta^{-1}$.

Let α be a sequence over G. The *length* of α, denoted by $|\alpha|$, is the total number of its terms (multiplicities are counted). The *support* of α, denoted by $supp(\alpha)$, is its underlying set: $supp(\alpha) = \{a \in G \mid \alpha \text{ has a term equal to } a\}$. The *sum* of α, denoted by $S(\alpha)$, is the sum of its terms. The *sumset* of α is defined to be the set $\Sigma(\alpha) = \{S(\beta) \mid \beta \text{ is a nonempty subsequence of } \alpha\}$. Sometimes we need the extended sumset $\Sigma^*(\alpha) = \Sigma(\alpha) \cup \{0\}$.

By definition the empty sequence $\varnothing$ has length $|\varnothing| = 0$, sum $S(\varnothing) = 0$, and satisfies $\Sigma(\varnothing) = supp(\varnothing) = \varnothing$.

A sequence α over G is:

- *zero-sum-free* if $0 \notin \Sigma(\alpha)$, i.e., if $S(\beta) \neq 0$ for each nonempty subsequence β of α;
- a *zero-sum sequence* if $S(\alpha) = 0$;
- a *minimal zero-sum sequence* if $\alpha \neq \varnothing$, $S(\alpha) = 0$, and $S(\beta) \neq 0$ for each proper nonempty subsequence β of α.

The subgroup generated by the support $supp(\alpha)$ of a sequence α over G is denoted by $\langle\alpha\rangle$, just like $\langle u\rangle$ is the subgroup generated by $\{u\}$, for $u \in G$. The meaning of $\langle u, v\rangle$, $\langle u, v, w\rangle$, etc., is analogous. For a subset A of G and $u \in G$, we define $u + A$ by $u + A = \{u + a \mid a \in A\}$. Sometimes $u + A$ is called a *translate* of A.

We will use the following notations for discrete intervals between integers a and b: $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$, $(a, b) = \{x \in \mathbb{Z} \mid a < x < b\}$, and others like $[a, b)$ are defined analogously.

2.1. Unsplittable and Admissible Sequences

The notion of an unsplittable sequence was introduced by Gao [1].

Definition 1. A minimal zero-sum sequence α over G is *unsplittable* if replacing any term t of α by any two elements of G with sum t yields a zero-sum sequence that is not minimal.

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

Lemma 1 ([6], Lemma 2.2; [4], Lemma 2.3)**.** *Let α be an unsplittable minimal zero-sum sequence over G, and let a be a term of α with multiplicity m_a. Then α has no term of the form ka with $k \in [2, m_a{+}1]$.*

Lemma 2 ([4], Lemma 2.4)**.** *Let α be a minimal zero-sum sequence over G. The following properties are equivalent:*

(i) α *is unsplittable;*

(ii) for each $a \in supp(\alpha)$*, one has* $\Sigma(\alpha a^{-1}) = G^{\bullet}$*;*

(iii) for each $a \in supp(\alpha)$ *and each* $g \in G$*, there is a subsequence of* α *that contains* a *and has sum* g*.*

We will study sequences of the following form and determine when they are unsplittable minimal zero-sum sequences.

Definition 2. A sequence α over G is called *admissible* if there exists a term $a \in supp(\alpha)$ with multiplicity m_a such that $\alpha = a^{m_a}\beta$, $\beta \neq \varnothing$, and $b - b' = xa$ with $x \in [-m_a, m_a]$ for all terms b and b' of β.

It is natural to consider such sequences due to the following reasons. The simplest kind of unsplittable minimal zero-sum sequences are of the form a^{m_a}, which can exist only in a finite cyclic group C_n where $C_n = \langle a \rangle$ and $n = m_a$. Next, we consider unsplittable sequences of the form $a^{m_a}\beta$ where $\beta \neq \varnothing$. The sumset $\Sigma(a^{m_a})$ is a progression with difference a. Due to minimality and unsplittability, for any $b \in \beta$, the translate $b + \Sigma^*(a^{m_a})$ must be a new progression disjoint from $\Sigma(a^{m_a})$. So it seems that the next simplest kind of unsplittable sequences is when the translates pairwise intersect, in other words, $(b + \Sigma^*(a^{m_a})) \cap (b' + \Sigma^*(a^{m_a})) \neq \varnothing$, for all terms b and b' of β. This is the motivation of Definition 2. In a finite cyclic group C_n, all unsplittable sequences of length at least $\lfloor n/3 \rfloor + 3$ ($n \geq 10$) turn out to be of the simplest or the admissible kind [4]. Most of the interesting unsplittable sequences known so far are also admissible (see [4, 7, 8, 9]). On the other hand, groups that allow unsplittable minimal zero-sum sequences of the admissible kind must either be cyclic or of rank 2.

2.2. 2-thread Sequences

We will see that unsplittable sequences of the admissible kind are in a special shape, which will be called 2-*thread*. The name attempts to indicate that such a sequence can be described by 2 terms.

Definition 3. A sequence α over G is called a 2-*thread* sequence if it has a representation of the form $\alpha = a^p b^q b_1 \cdots b_k$ where:

$$a \in G^{\bullet},\ b \in G,\ p \in (0, \mathrm{ord}(a));\ q, k \in \mathbb{Z},\ q \geq 0,\ k \geq 2;\ b_1 = b,\ b_k \neq b;$$
$$b_j = b - s_j a \text{ with } s_j \in [0, p] \text{ for } j \in [1, k]; \text{ and } kb = (s_1 + \cdots + s_k + 1)a.$$

Remark 1. The notation in Definition 3 is always assumed for a 2-thread sequence α. Note that the definition does not state that p must equal the multiplicity of a in α. On the other hand, every 2-thread sequence is clearly admissible.

In some cases additional notation is necessary or convenient. We introduce it below and use it repeatedly in the sequel without explanation whenever appropriate.

Let $\alpha = a^p b^q b_1 \cdots b_k$ be a 2-thread sequence.

- Denote $s = s_1 + \cdots + s_k$; then the condition $kb = (s_1 + \cdots + s_k + 1)a$ takes the form $kb = (s+1)a$. It is also equivalent to $b_1 + \cdots + b_k = a$. Note in addition that $b_1 = b$ and $b_k \neq b$ mean $s_1 = 0$ and $s_k \neq 0$ respectively.
- Set $\sigma = b_1 \cdots b_k | \alpha$; then $S(\sigma) = a$, and $\alpha = a^p b^q b_1 \cdots b_k$ can be shortened to $\alpha = a^p b^q \sigma$. The terms of σ are not all equal as $b_1 \neq b_k$.
- Define $\sigma_0 = \varnothing$, $t_0 = 0$; and $\sigma_i = b_1 \cdots b_i$, $t_i = s_1 + \cdots + s_i$ for $i \in [1, k]$. Note that $\sigma_k = \sigma$ and $t_k = s$.
- We need parameters not present in Definition 3 already for the statement of the main result. Moreover they are essential for the exposition.

  Denote by r the least nonnegative remainder of q modulo k, and by d the greatest common divisor of q and k. Then $d = \gcd(k, r)$; set $k = dk'$, $r = dr'$, where $\gcd(k', r') = 1$.

Theorem 2. *The following statements are equivalent for a sequence α over G.*

(1) α is an admissible and unsplittable minimal zero-sum sequence.

(2) α is a 2-thread sequence with sum 0 satisfying the following conditions:

(a) the factor group $G/\langle a \rangle$ is cyclic of order d and generated by the a-coset $b + \langle a \rangle$;

(b) $k(p+1) + q(s+1) = |G|$.

It is worth noting that the proof of Theorem 2 would have been much shorter and transparent if additional assumptions were made, e.g., $s \leq p$ or $q \geq k$. Without such restrictions we need to have a better understanding of 2-thread sequences.

3. On 2-thread Sequences with Sum Zero

In this section we study 2-thread sequences with sum 0. The goal is Proposition 1, which will be used in the proof of Theorem 2.

3.1. An Independent Observation about Integers

Lemma 3. *Let $k, r \in \mathbb{Z}$, $k \geq 2$, and $0 \leq r < k$. Set $d = \gcd(k, r)$ and $k = dk'$. For $j \in [0, k']$, let r_j be the least nonnegative remainder of jr modulo k. Then:*

a) $r_0, r_1, \ldots, r_{k'-1}$ *is a permutation of* $0, d, \ldots, (k'-1)d$;

b) for $j \in [0, k'-1]$,

$$r_{j+1} = r_j + r \text{ if } r_{j+1} \geq r; \qquad r_{j+1} = r_j + r - k \text{ if } r_{j+1} < r. \tag{1}$$

Proof. a) Since $d = \gcd(k, r)$, let us set $r = dr'$ with $\gcd(k', r') = 1$. Then $0, r', \ldots, (k'-1)r'$ is a complete set of residues modulo k'. Therefore the integers $0, dr', \ldots, (k'-1)dr'$, i.e., $0, r, \ldots, (k'-1)r$, are all divisible by d and different modulo $dk' = k$. Moreover, $0, r, \ldots, (k'-1)r$ represent exactly once every congruence class modulo k that consists of multiples of d. Hence $r_0, r_1, \ldots, r_{k'-1}$ is a permutation of $0, d, \ldots, (k'-1)d$.

b) For $j \in [0, k'-1]$, by definition $r_{j+1} \equiv r_j + r \pmod{k}$ and $r_j \in [0, k-1]$. It follows that either $r_{j+1} = r_j + r$ or $r_{j+1} = r_j + r - k$ according as $r_{j+1} \geq r$ or $r_{j+1} < r$. $\square$

Remark 2. The quantities r_j play an important rôle in the sequel. They are always assumed to be defined as in Lemma 3, hence they satisfy the relations in (1). Observe also that $r_1 = r$ and $r_{k'} = r_0 = 0$ by definition.

If $r = 0$, then $d = k$ and $k' = 1$. If $r \neq 0$, then $d \leq r < k$ and $k' \geq 2$. By $r_{k'} = r_0$ and Lemma 3a, $r_1, \ldots, r_{k'}$ is a permutation of $0, d, \ldots, (k'-1)d$. In particular, $r_j \neq r$ if $j \in [2, k']$, and $r_j \in [d, k-d]$ for $j \in [1, k'-1]$. Moreover, $r_{k'-1} = k - r$.

We state a simple corollary of Lemma 3 about 2-thread sequences with sum 0.

Lemma 4. *Let* $\alpha = a^p b^q \sigma$ *be a* 2*-thread sequence over* G *with sum* 0. *Set* $q = mk + r$ *with* $r \in [0, k-1]$ *and* $\ell = m(s+1) + p + 1$. *Then* $qb = -(p+1)a$, $rb = -\ell a$, *and for* $j \in [0, k'-1]$,

$$r_{j+1}b = r_j b - \ell a \text{ if } r_{j+1} \geq r; \qquad r_{j+1}b = r_j b - (\ell + s + 1)a \text{ if } r_{j+1} < r. \tag{2}$$

Proof. By $S(\alpha) = 0$ and $S(\sigma) = a$, we have $qb = -(p+1)a$. This can be written as $rb = -\ell a$ since $kb = (s+1)a$. Then the relations in (2) follow from those in (1). $\square$

3.2. Progressions in the Sumsets of 2-thread Sequences with Sum 0

By Lemma 4, for a 2-thread sequence with sum 0, $r_j b \in \langle a \rangle$ for all $j \in [0, k'-1]$; and the relations in (2) seem to suggest a decreasing order. However, without knowing the structure of G (e.g., order of a), it is not clear how $r_j b$'s are located in $\langle a \rangle$. To investigate further, let us define the following notions.

Definition 4. Let $a \in G^\bullet$ and $g \in \langle a \rangle$. We denote by $x_a(g)$ the unique integer in $[1, \mathrm{ord}(a)]$ such that $g = x_a(g)a$ and call it the *a-coordinate of g*.

Definition 5. An arithmetic progression in G with common difference $a \in G^\bullet$ will be called an *a-progression*. Let $u \in G$ and $a \in G^\bullet$. If $v = u + La$ with $L \in \mathbb{Z}$ and $L \geq 0$, then the collection of all $u+xa$ with $x \in [0, L]$ is $[u, v]_a^L = \{u+xa | x \in [0, L]\}$, and will be called an *a-progression with length L starting at u*. In a group, this is possibly a multiset (with repetitions). We will say that $[u, v]_a^L$ is contained in a sumset Σ and write $[u, v]_a^L \subseteq \Sigma$ if every term in the length L a-progression $[u, v]_a^L$ is in Σ, i.e., $u + xa \in \Sigma$ for all $x \in [0, L]$. Clearly, if $[u, v]_a^{L_1} \subseteq \Sigma$ and $[v, w]_a^{L_2} \subseteq \Sigma$, then $[u, w]_a^{L_1+L_2} \subseteq \Sigma$.

Proposition 1 states that for a 2-thread sequence α with sum 0, certain a-progressions with appropriate lengths are in the sumset $\Sigma(\alpha t^{-1})$, where t is any term of α. To build up to the proof, we need several lemmas. First, we define an operation that will be applied repeatedly.

Definition 6. Let $a^p\beta$ be a sequence over G where $a \in G^\bullet$, $p \in \mathbb{Z}$, $p \geq 0$, $\beta \neq \varnothing$, and let τ be a nonempty subsequence of β. Suppose that $c \in \tau$ and $c' \in \beta\tau^{-1}$ satisfy $c = c' - sa$ with $s \in [0, p]$. Then we say that the subsequence $\tau' = \tau c^{-1} c' | \beta$ can be obtained from τ by an *elementary a-swap* with a step-size of s. Furthermore, we write $\tau \xrightarrow{a,I} \tau'$ if τ' can be obtained from τ by several elementary a-swaps, and I is the sum of the step-sizes of the swaps. We will shorten an a-swap to a swap and write $\tau \xrightarrow{I} \tau'$ whenever a is clear.

The following simple lemma reveals a connection between elementary a-swaps and a-progressions in a sumset.

Lemma 5. *Let $a^p\beta$ be a sequence over G where $a \in G^\bullet$, $p \in \mathbb{Z}$, $p \geq 1$, and $\beta \neq \varnothing$. Let τ, τ' be subsequences of β such that $\tau \xrightarrow{a,I} \tau'$. Then the a-progression $[S(\tau), S(\tau')]_a^I$ is contained in the sumset $\Sigma(a^{p-1}\beta)$.*

Proof. By the last remark in Definition 5, it suffices to prove the claim in the case when τ' is obtained from τ by a single swap. Let $\tau' = \tau c^{-1} c'$ where $c \in \tau$, $c' \in \beta\tau^{-1}$, and $c = c' - sa$ with $s \in [0, p]$. Then $S(\tau') = S(\tau) - c + c' = S(\tau) + sa$. If $s = 0$, then $S(\tau') = S(\tau) \in \Sigma(\beta)$ and the conclusion holds trivially. Let $s \in [1, p]$. Clearly, the a-progression $P = [S(\tau), S(\tau) + (p-1)a]_a^{p-1}$ is contained in $\Sigma(a^{p-1}\beta)$. Notice that $S(\tau') - a = S(\tau) + (s-1)a \in P$. As $S(\tau') \in \Sigma(\beta)$, it follows that $[S(\tau), S(\tau')]_a^s \subseteq \Sigma(a^{p-1}\beta)$. □

Let α be a 2-thread sequence with sum 0; recall notations from Definition 3 and Remark 1. Remove a term $t \in \alpha$ and consider the sumset $\Sigma(\alpha t^{-1})$. We state several lemmas about the a-progressions contained in such a sumset. The first one is about $\Sigma(\alpha a^{-1})$.

Lemma 6. *Let $\alpha = a^p b^q \sigma$ be a 2-thread sequence over G with sum 0. Then $[S(b^q\sigma_i), S(\sigma_i)]_a^{p+1} \subseteq \Sigma(\alpha a^{-1})$ for each $i \in [1, k-1]$.*

Proof. For each $i \in [1, k-1]$, $b^q\sigma_i | b^q\sigma$ is a nonempty subsequence. Clearly, we have $[S(b^q\sigma_i), S(b^q\sigma_i) + (p-1)a]_a^{p-1} \subseteq \Sigma(\alpha a^{-1})$. Now $S(\alpha) = 0$ and $S(\sigma) = a$ imply that $qb = -(p+1)a$. So $S(b^q\sigma_i) + (p-1)a = S(\sigma_i) + qb + (p-1)a = S(\sigma_i) - 2a$, and hence $[S(b^q\sigma_i), S(\sigma_i) - 2a]_a^{p-1} \subseteq \Sigma(\alpha a^{-1})$. As $\sigma_i | \sigma$ is a nonempty subsequence, $S(\sigma_i) \in \Sigma(\alpha a^{-1})$. It remains to show that $S(\sigma_i) - a \in \Sigma(\alpha a^{-1})$.

Recall $b_k = b_1 - s_k a$ with $s_k \in [1, p]$; and that for each $i \in [1, k-1]$, $b_1 \in \sigma_i$ and $b_k \notin \sigma_i$. Let $\sigma_i' = \sigma_i b_1^{-1} b_k$. Since $\sigma_i' | \sigma$ is a nonempty subsequence, we have $P = [S(\sigma_i'), S(\sigma_i') + (p-1)a]_a^{p-1} \subseteq \Sigma(\alpha a^{-1})$. Note that $S(\sigma_i') = S(\sigma_i) - b_1 + b_k = S(\sigma_i) - s_k a$, which implies $S(\sigma_i) - a = S(\sigma_i') + (s_k - 1)a$. As $s_k - 1 \in [0, p-1]$, we obtain $S(\sigma_i) - a \in P \subseteq \Sigma(\alpha a^{-1})$ as desired. □

Remark 3. In fact, the conclusion in Lemma 6 holds for any nonempty proper subsequence $\gamma | \sigma$, i.e., $[S(b^q\gamma), S(\gamma)]_a^{p+1} \subseteq \Sigma(\alpha a^{-1})$.

Given a 2-thread sequence $\alpha = a^p b^q \sigma$ with sum 0, relations in (2) imply that for $j \in [0, k'-1]$, $r_j b = r_{j+1} b + La$ where $L = \ell$ or $\ell + s + 1$. In the more substantial case when $q \geq 1$, we consider $P_j = [r_{j+1}b, r_j b]_a^L = \{r_{j+1}b + xa | x \in [0, L]\}$, and will show that these a-progressions and certain translates are essentially in the sumset of α with any term t removed ($\Sigma(\alpha t^{-1})$). The precise statements are in Proposition 1.

The following two lemmas are the main ingredients in the proof of Proposition 1. Despite being lengthy, the arguments are mostly calculations based on simple ideas. We will handle the cases $q \geq k$ and $q < k$ separately. When $q \geq k$, the lengths of P_j's are ℓ or $\ell + s + 1$, where $\ell = m(s+1) + p + 1$ with $m \geq 1$. Each progression P_j can be regarded as a concatenation of segments of lengths $s+1$ and a last stretch of length $p + s + 2$. Lemma 7 shows that these pieces are in $\Sigma(\alpha t^{-1})$. The case $q < k$ ($q = r$) is a little complicated. We use other considerations in Lemma 8.

Lemma 7. *Let $\alpha = a^p b^q \sigma$ be a 2-thread sequence over G with $q \geq k$ and sum 0. Let $t \in supp(\alpha)$ and denote $\Sigma(\alpha t^{-1}) = \Sigma$. Then the following statements hold.*

a) If $R \in [k, q]$, then $[(R-k)b + a, Rb]_a^s \subseteq \Sigma$.

b) For $j \in [0, k'-1]$ and $\lambda \in [0, d-1]$ with $\lambda + r_j \neq 0$,

$$[(\lambda + r_j)b - (p+s+2)a, (\lambda + r_j)b]_a^{p+s+2} \subseteq \Sigma.$$

Proof. Let $t \in supp(\alpha)$, then $t = a$ or $t \in supp(b^q\sigma)$. The proofs of the two cases are similar. We consider $t = a$ here and leave the case $t \in supp(b^q\sigma)$ to Appendix A.

In the following $t = a$ and $\Sigma = \Sigma(\alpha a^{-1})$. Let $\beta = b^q\sigma$, then $\alpha a^{-1} = a^{p-1}\beta$. For the 2-thread sequence $\alpha = a^p\beta$, recall the notations in Definition 3, Remark 1, and define elementary a-swaps as in Definition 6.

a) Since $R \in [k, q]$, the subsequences $b^{R-k}\sigma$ and b^R of β are nonempty. Notice that $b^{R-k}\sigma \xrightarrow{s} b^R$, as the latter can be obtained from the former by k elementary swaps, each time replacing a term in σ by a b in $b^q(b^{R-k})^{-1}$. Lemma 5 implies that $[S(b^{R-k}\sigma), S(b^R)]_a^s \subseteq \Sigma(a^{p-1}\beta)$, that is, $[(R-k)b+a, Rb]_a^s \subseteq \Sigma$.

b) Note that $\lambda + r_j \in [1, k-1]$, as $\lambda + r_j \neq 0$, $\lambda \in [0, d-1]$, and $r_j \in [0, k-d]$.

Observe that $b^{\lambda+r_j+q-k}\sigma \xrightarrow{I} b^q\sigma_{\lambda+r_j}$ with $I = s - t_{\lambda+r_j}$, as both are nonempty subsequences of β, and the latter can be obtained from the former by $k-(\lambda+r_j)$ elementary swaps, each time replacing a term in $\sigma(\sigma_{\lambda+r_j})^{-1}$ by a b in $b^q(b^{\lambda+r_j+q-k})^{-1}$. Hence $[S(b^{\lambda+r_j+q-k}\sigma), S(b^q\sigma_{\lambda+r_j})]_a^I \subseteq \Sigma(a^{p-1}\beta)$ (Lemma 5). Next, by Lemma 6 $[S(b^q\sigma_{\lambda+r_j}), S(\sigma_{\lambda+r_j})]_a^{p+1} \subseteq \Sigma(\alpha a^{-1})$. Finally, $\sigma_{\lambda+r_j} \xrightarrow{t_{\lambda+r_j}} b^{\lambda+r_j}$, as both are nonempty subsequences of β and the latter can be obtained from the former by $\lambda + r_j$ elementary swaps replacing the terms in $\sigma_{\lambda+r_j}$ by b's in b^q. Therefore $[S(\sigma_{\lambda+r_j}), S(b^{\lambda+r_j})]_a^{t_{\lambda+r_j}} \subseteq \Sigma(a^{p-1}\beta)$ (Lemma 5).

Combining the three progressions, we have $[S(b^{\lambda+r_j+q-k}\sigma), S(b^{\lambda+r_j})]_a^{p+s+1} \subseteq \Sigma$, where the length equals $I+(p+1)+t_{\lambda+r_j} = p+s+1$. Since $S(b^{\lambda+r_j+q-k}) \in \Sigma(b^q)$ and $S(b^{\lambda+r_j+q-k}\sigma) = S(b^{\lambda+r_j+q-k}) + a$, we have $[S(b^{\lambda+r_j+q-k}), S(b^{\lambda+r_j})]_a^{p+s+2} \subseteq \Sigma$. Computing the sums at the ends of the progression, and recalling that $kb = (s+1)a$ and $qb = -(p+1)a$, we obtain $[(\lambda + r_j)b - (p+s+2)a, (\lambda + r_j)b]_a^{p+s+2} \subseteq \Sigma$. $\square$

Lemma 8. *Let $\alpha = a^p b^q \sigma$ be a 2-thread sequence over G with $q = r \geq 1$ and sum 0. Let $t \in supp(\alpha)$ and denote $\Sigma(\alpha t^{-1}) = \Sigma$. Then the following hold.*

a) $[r_1 b, -a]_a^p \subseteq \Sigma$; and in the case $d \geq 2$, $[(\lambda + r_1)b, \lambda b]_a^{p+1} \subseteq \Sigma$ for $\lambda \in [1, d-1]$.

b) For $j \in [1, k'-1]$ and $\lambda \in [0, d-1]$,

- *if $\lambda + r_{j+1} \neq 0$, then $[(\lambda + r_{j+1})b, (\lambda + r_j)b]_a^L \subseteq \Sigma$, where $L = p+1$ if $r_{j+1} > r$ or $L = p+s+2$ if $r_{j+1} < r$;*
- *if $\lambda + r_{j+1} = 0$ (which happens when $\lambda = 0$ and $j = k'-1$), then $[(\lambda + r_{j+1})b + a, (\lambda + r_j)b]_a^{p+s+1} \subseteq \Sigma$, in other words, $[a, r_{k'-1}b]_a^{p+s+1} \subseteq \Sigma$.*

Proof. Let $t \in supp(\alpha)$. Like in the proof of Lemma 7, the two cases $t = a$ and $t \in supp(b^q\sigma)$ are similar; we consider $t = a$ here and leave $t \in supp(b^q\sigma)$ to Appendix A.

In the following, $t = a$ and $\Sigma = \Sigma(\alpha a^{-1})$. As $S(\alpha) = 0$ and $q = r$, $rb = -(p+1)a$. Let $\beta = b^r\sigma$, then $\alpha a^{-1} = a^{p-1}\beta$. For the 2-thread sequence α, recall the notations in Definition 3, Remark 1, and define elementary a-swaps as in Definition 6. Note that $r_1 = r$ (Remark 2), and $r \neq 0$ implies $d \leq r$.

a) Clearly, $[S(b^r), S(b^r) + (p-1)a]_a^{p-1} \subseteq \Sigma$, i.e., $[r_1 b, -2a]_a^{p-1} \subseteq \Sigma$. Since $S(\alpha a^{-1}) = -a$, the desired $[r_1 b, -a]_a^p \subseteq \Sigma$ follows.

Suppose $d \geq 2$. Then for $\lambda \in [1, d-1]$, $\lambda \leq d-1 \leq r-1 \leq k-1$. Observe that $\sigma_\lambda \xrightarrow{t_\lambda} b^\lambda$, as both are nonempty subsequences of β and the latter can be obtained from the former by λ elementary swaps, each time replacing a term in σ_λ by a b in b^r. Hence $[S(\sigma_\lambda), S(b^\lambda)]_a^{t_\lambda} \subseteq \Sigma$ (Lemma 5). On the other hand, $[S(b^r\sigma_\lambda), S(\sigma_\lambda)]_a^{p+1} \subseteq \Sigma$ (Lemma 6). Therefore $P = [S(b^r\sigma_\lambda), S(b^\lambda)]_a^I \subseteq \Sigma$, where $I = p+1+t_\lambda$. By computation, we have $S(b^r\sigma_\lambda) = (\lambda+r)b - t_\lambda a$ and $S(b^\lambda) = \lambda b = (\lambda+r)b+(p+1)a$. As $t_\lambda \geq 0$, $(\lambda+r)b \in P$. Hence $[(\lambda+r_1)b, \lambda b]_a^{p+1} \subseteq \Sigma$ for $\lambda \in [1, d-1]$ as desired. We state an additional result that will be used later:

$$[S(b^r\sigma_\lambda), (\lambda+r_1)b]_a^{t_\lambda} \subseteq \Sigma, \quad \text{for } \lambda \in [0, d-1]. \tag{3}$$

Note that (3) follows from the above when $\lambda \in [1, d-1]$, and it holds trivially for $\lambda = 0$ (recall $\sigma_0 = \varnothing$ and $t_0 = 0$).

b) By Remark 2, $r_{k'} = r_0 = 0$, and for $j \in [1, k'-1]$, $r_j \in [d, k-d]$ and $r_{j+1} \in [0, k-d]$; hence $\lambda + r_j \in [d, k-1]$ and $\lambda + r_{j+1} \in [0, k-1]$ (as $\lambda \in [0, d-1]$). We will prove the following stronger statement.

Claim 1. *For $j \in [1, k'-1]$ and $\lambda \in [0, d-1]$,*

- *if $r_{j+1} > r$, then $[(\lambda+r_{j+1})b - t_{\lambda+r_j}a, (\lambda+r_j)b]_a^L \subseteq \Sigma$ with $L = p+1+t_{\lambda+r_j}$;*
- *if $r_{j+1} < r$, then $[(\lambda+r_{j+1})b + a, (\lambda+r_j)b]_a^{p+s+1} \subseteq \Sigma$.*

Let us first show that part (b) follows from the claim. Suppose $\lambda + r_{j+1} \neq 0$. If $r_{j+1} > r$, then $r_{j+1} = r_j + r$ (Lemma 3b), hence $(\lambda+r_j)b = (\lambda+r_{j+1})b + (p+1)a$. By the claim, $P = [(\lambda+r_{j+1})b - t_{\lambda+r_j}a, (\lambda+r_j)b]_a^L \subseteq \Sigma$ with $L = p+1+t_{\lambda+r_j}$. As $t_{\lambda+r_j} \geq 0$, $(\lambda+r_{j+1})b \in P$. Hence $[(\lambda+r_{j+1})b, (\lambda+r_j)b]_a^{p+1} \subseteq \Sigma$ as desired. If $r_{j+1} < r$, then $0 \leq r_{j+1} \leq r-d$ since both r_{j+1} and r are multiples of d (Lemma 3a). As $\lambda \in [0, d-1]$ and $\lambda + r_{j+1} \neq 0$, $\lambda + r_{j+1} \in [1, r-1]$. So $(\lambda+r_{j+1})b = S(b^{\lambda+r_{j+1}}) \in \Sigma(b^r)$. By the claim, $[(\lambda+r_{j+1})b+a, (\lambda+r_j)b]_a^{p+s+1} \subseteq \Sigma$. Therefore $[(\lambda+r_{j+1})b, (\lambda+r_j)b]_a^{p+s+2} \subseteq \Sigma$. Suppose $\lambda + r_{j+1} = 0$, then $\lambda = 0$ and $j = k'-1$. As $r_{j+1} = r_{k'} = 0 < r$, the claim implies $[a, r_{k'-1}b]_a^{p+s+1} \subseteq \Sigma$.

Before proving Claim 1, we show by induction on j that for $j \in [1, k'-1]$ and $\lambda \in [0, d-1]$,

$$[S(\sigma_{\lambda+r_j}), (\lambda+r_j)b]_a^{t_{\lambda+r_j}} \subseteq \Sigma. \tag{4}$$

For the base case, let $j = 1$ and $\lambda \in [0, d-1]$. Note that $r_1 = r$ and $\lambda + r \in [1, k-1]$. Observe $\sigma_{\lambda+r} \xrightarrow{J} b^r\sigma_\lambda$ with $J = t_{\lambda+r} - t_\lambda$, as both are nonempty subsequences of β and the latter can be obtained from the former by r elementary swaps, replacing the terms in $\sigma_{\lambda+r}(\sigma_\lambda)^{-1}$ by b^r. Hence $[S(\sigma_{\lambda+r}), S(b^r\sigma_\lambda)]_a^J \subseteq \Sigma$ (Lemma 5). Together with the result in (3), the desired $[S(\sigma_{\lambda+r_1}), (\lambda+r_1)b]_a^{t_{\lambda+r_1}} \subseteq \Sigma$ follows.

For the inductive step $j \mapsto j+1$, where $j \in [1, k'-2]$, note that $j+1 \in [2, k'-1]$, so $r_j, r_{j+1} \in [d, k-d]$ and $\lambda + r_j, \lambda + r_{j+1} \in [1, k-1]$. We need to show that

$$[S(\sigma_{\lambda+r_{j+1}}), (\lambda+r_{j+1})b]_a^{t_{\lambda+r_{j+1}}} \subseteq \Sigma. \tag{5}$$

If $r_{j+1} < r$, then $\lambda + r_{j+1} \in [1, r-1]$, since both r_{j+1} and r are multiples of d and $\lambda \in [0, d-1]$. Clearly $\sigma_{\lambda+r_{j+1}} \xrightarrow{t_{\lambda+r_{j+1}}} b^{\lambda+r_{j+1}}$, as both are nonempty subsequences of β and the latter can be obtained from the former by $\lambda + r_{j+1}$ elementary swaps, each time replacing a term in $\sigma_{\lambda+r_{j+1}}$ by a b in b^r. By Lemma 5, the desired (5) follows.

If $r_{j+1} > r$ then $r_{j+1} = r_j + r$. We know $[S(\sigma_{\lambda+r_j}), (\lambda + r_j)b]_a^{t_{\lambda+r_j}} \subseteq \Sigma$ (inductive hypothesis), and $[S(b^r\sigma_{\lambda+r_j}), S(\sigma_{\lambda+r_j})]_a^{p+1} \subseteq \Sigma$ (Lemma 6). Therefore $Q = [S(b^r\sigma_{\lambda+r_j}), (\lambda + r_j)b]_a^{J_1} \subseteq \Sigma$, where $J_1 = p + 1 + t_{\lambda+r_j}$. By computation, $S(b^r\sigma_{\lambda+r_j}) = (\lambda+r_{j+1})b - t_{\lambda+r_j}a$ and $(\lambda+r_j)b = (\lambda+r_{j+1})b+(p+1)a$. As $t_{\lambda+r_j} \geq 0$, we have that $(\lambda + r_{j+1})b$ is in Q, and so $Q_1 = [S(b^r\sigma_{\lambda+r_j}), (\lambda + r_{j+1})b]_a^{t_{\lambda+r_j}} \subseteq \Sigma$. On the other hand, $\sigma_{\lambda+r_{j+1}} \xrightarrow{J_2} b^r\sigma_{\lambda+r_j}$ with $J_2 = t_{\lambda+r_{j+1}} - t_{\lambda+r_j}$, as both are nonempty subsequences of β and the latter can be obtained from the former by r elementary swaps replacing the terms in $\sigma_{\lambda+r_{j+1}}(\sigma_{\lambda+r_j})^{-1}$ by b^r. Hence $Q_2 = [S(\sigma_{\lambda+r_{j+1}}), S(b^r\sigma_{\lambda+r_j})]_a^{J_2} \subseteq \Sigma$ (Lemma 5). Combining Q_2 and Q_1, the desired (5) follows. This completes the induction and the proof of (4).

Now we are ready to prove Claim 1. Let $j \in [1, k' - 1]$ and $\lambda \in [0, d - 1]$. Note that $\lambda + r_j \in [1, k - 1]$. By Lemma 6, $[S(b^r\sigma_{\lambda+r_j}), S(\sigma_{\lambda+r_j})]_a^{p+1} \subseteq \Sigma$. Together with (4), we obtain

$$[S(b^r\sigma_{\lambda+r_j}), (\lambda + r_j)b]_a^{p+1+t_{\lambda+r_j}} \subseteq \Sigma. \tag{6}$$

If $r_{j+1} > r$, then (6) is what is desired, since $S(b^r\sigma_{\lambda+r_j}) = (\lambda + r_{j+1})b - t_{\lambda+r_j}a$. If $r_{j+1} < r$, then $r_{j+1} = r_j + r - k$ (Lemma 3b), meaning $k - r_j = r - r_{j+1}$. Note that $b^{\lambda+r_{j+1}}\sigma \xrightarrow{H} b^r\sigma_{\lambda+r_j}$ with $H = s - t_{\lambda+r_j}$, since both are nonempty subsequences of β ($\lambda + r_{j+1} \in [0, r - 1]$), and the latter can be obtained from the former by $k - (\lambda + r_j)$ elementary swaps, each time replacing a term in $\sigma(\sigma_{\lambda+r_j})^{-1}$ by a b in $b^r(b^{\lambda+r_{j+1}})^{-1}$. This is possible since $k - (\lambda + r_j) = r - (\lambda + r_{j+1})$. Hence $[S(b^{\lambda+r_{j+1}}\sigma), S(b^r\sigma_{\lambda+r_j})]_a^H \subseteq \Sigma$ (Lemma 5). Together with (6), we obtain $[S(b^{\lambda+r_{j+1}}\sigma), (\lambda+r_j)b]_a^{p+s+1} \subseteq \Sigma$, where the length is $H+(p+1+t_{\lambda+r_j}) = p+s+1$. Since $S(b^{\lambda+r_{j+1}}\sigma) = (\lambda+r_{j+1})b+a$, the desired $[(\lambda+r_{j+1})b+a, (\lambda+r_j)b]_a^{p+s+1} \subseteq \Sigma$ follows. This completes the proof of Claim 1 and the lemma. $\square$

Remark 4. Notice that in part (b) of Lemma 8, there is no need to consider the case $r_{j+1} = r$ since $r_{j+1} \neq r$ for $j \in [1, k' - 1]$ (Remark 2).

We are ready to present the main result of the section. Here is an explanation for the organization of the statements in Proposition 1. When $r = 0$, only $r_0 = 0$ is present in the sequence $r_0, \ldots, r_{k'-1}$ (as $d = k$ and $k' = 1$); and $d \geq 2$ since $k \geq 2$ is assumed for 2-thread sequences. Suppose $r \neq 0$; then $d < k$ and $k' \geq 2$. In the sequence $r_0, \ldots, r_{k'-1}$, at least r_0 and $r_{k'-1}$ are present; and results about them are in part (b)(i,ii). If $k' \geq 3$, then part (b)(iii) is about r_j's for $j \in [1, k' - 2]$. The cases of $q = r < k$ and $q \geq k$ will be handled separately. The former was essentially done in Lemma 8. For the latter we will use Lemma 7 repeatedly.

Proposition 1. *Let $\alpha = a^p b^q \sigma$ be a 2-thread sequence over G with $q \geq 1$ and sum 0. Set $q = mk + r$ with $r \in [0, k-1]$ and $\ell = m(s+1) + p + 1$. Let $t \in supp(\alpha)$, denote $\Sigma(\alpha t^{-1}) = \Sigma$. Then the following statements hold.*

a) If $r = 0$, then $[a, -a]_a^{\ell-2} \subseteq \Sigma$, and $\lambda b + \langle a \rangle \subseteq \Sigma$ for $\lambda \in [1, d-1]$.

b) If $r \neq 0$, then:

- *(i) $[r_1 b, -a]_a^{\ell-1} \subseteq \Sigma$; and in the case $d \geq 2$, $[(\lambda + r_1)b, \lambda b]_a^{\ell} \subseteq \Sigma$ for $\lambda \in [1, d-1]$;*
- *(ii) $[a, r_{k'-1} b]_a^{\ell+s} \subseteq \Sigma$; and in the case $d \geq 2$, $[\lambda b, (\lambda + r_{k'-1})b]_a^{\ell+s+1} \subseteq \Sigma$ for $\lambda \in [1, d-1]$;*
- *(iii) if $k' \geq 3$, then $[(\lambda + r_{j+1})b, (\lambda + r_j)b]_a^{L} \subseteq \Sigma$ for $j \in [1, k'-2]$ and $\lambda \in [0, d-1]$, where $L = \ell$ if $r_{j+1} > r$ or $L = \ell + s + 1$ if $r_{j+1} < r$.*

Proof. As $q = mk + r$ with $m \geq 0$, we consider two cases.

Case 1: $m = 0$. In this case, $q = r \geq 1$ and $\ell = p + 1$. In particular $r \neq 0$. Part (b) follows from Lemma 8. Indeed, (b)(i) is Lemma 8a; (b)(ii) follows from Lemma 8b by letting $j = k' - 1$ and noticing that $r_{j+1} = r_{k'} = 0 < r$; and (b)(iii) follows from Lemma 8b.

Case 2: $m \geq 1$. Here $q \geq k$. As α is a 2-thread sequence with sum 0, we have

$$qb = -(p+1)a, \quad kb = (s+1)a, \quad rb = -\ell a.$$

Let $t \in supp(\alpha)$, then either $t = a$ or we may assume $t \in \sigma$ since there is at least one b in σ by Definition 3. Let us first prove part (a) and part (b)(i).

Notice that $[qb, -a]_a^p \subseteq \Sigma$. Indeed, if $t = a$, then $[qb, qb+(p-1)a]_a^{p-1} \subseteq \Sigma(a^{p-1}b^q)$, so $[qb, -2a]_a^{p-1} \subseteq \Sigma(\alpha a^{-1})$. Together with $S(\alpha a^{-1}) = -a$, we have $[qb, -a]_a^p \subseteq \Sigma$. If $t \in \sigma$, then $[qb, qb + pa]_a^p \subseteq \Sigma(a^p b^q)$, and hence $[qb, -a]_a^p \subseteq \Sigma$. On the other hand, for $i \in [1, m]$, $ik + r \in [k, q]$. By Lemma 7a, $[((i-1)k + r)b + a, (ik + r)b]_a^s \subseteq \Sigma$. Combining the progressions for $i \in [1, m]$, we obtain $[rb + a, (mk + r)b]_a^{m(s+1)-1} \subseteq \Sigma$, that is, $[rb + a, qb]_a^{\ell-p-2} \subseteq \Sigma$. It follows that $[rb + a, -a]_a^{\ell-2} \subseteq \Sigma$. If $r = 0$, then $[a, -a]_a^{\ell-2} \subseteq \Sigma$ as needed in part (a). If $r \neq 0$, then $rb \in \Sigma(b^q)$, and hence $[r_1 b, -a]_a^{\ell-1} \subseteq \Sigma$ as desired in part (b)(i).

If $d \geq 2$, then for $\lambda \in [1, d-1]$, $\lambda + r \in [1, k-1]$. As $q \geq k$, $(\lambda + r)b \in \Sigma(b^q)$. First, we show that $[(\lambda + r)b, ((m-1)k + \lambda + r)b]_a^{(m-1)(s+1)} \subseteq \Sigma$. This is trivial if $m = 1$. If $m \geq 2$, then for $i \in [1, m-1]$, $ik + \lambda + r \in [k, q]$. By Lemma 7a we have $[((i-1)k + \lambda + r)b + a, (ik + \lambda + r)b]_a^s \subseteq \Sigma$. Combining the progressions for $i \in [1, m-1]$ and recalling that $(\lambda + r)b \in \Sigma$, we obtain $[(\lambda + r)b, ((m-1)k + \lambda + r)b]_a^{(m-1)(s+1)} \subseteq \Sigma$. Notice that $(m-1)(s+1) = \ell - (p+s+2)$ and $((m-1)k + \lambda + r)b = \lambda b - (p+s+2)a$, hence $[(\lambda + r)b, \lambda b - (p+s+2)a]_a^{\ell-(p+s+2)} \subseteq \Sigma$. Apply Lemma 7b with $j = 0$ and $\lambda \in [1, d-1]$, we have $[\lambda b - (p+s+2)a, \lambda b]_a^{p+s+2} \subseteq \Sigma$. In summary, $[(\lambda + r)b, \lambda b]_a^{\ell} \subseteq \Sigma$ for $\lambda \in [1, d-1]$. When $r = 0$, the above argument implies that $\lambda b + \langle a \rangle \subseteq \Sigma$ for $\lambda \in [1, d-1]$.

So far we have shown part (a) and part (b)(i). It remains to show part (b)(ii,iii) in the case $m \geq 1$. Recall that when $r \neq 0$, $k > r \geq d$ and $k' \geq 2$. For $j \in [1, k'-1]$, $r_{j+1} \neq r$; we consider the cases $r_{j+1} < r$ and $r_{j+1} > r$ separately.

If $r_{j+1} < r$, then $r_{j+1} = r_j + r - k$. Note that $r_{j+1} \leq r - d$ (r_{j+1} and r are multiples of d). For $\lambda \in [0, d-1]$, $\lambda + r_{j+1} \in [0, r-1]$. Hence for $i \in [1, m]$, $ik + \lambda + r_{j+1} \in [k, q]$. By Lemma 7a, $[((i-1)k + \lambda + r_{j+1})b + a, (ik + \lambda + r_{j+1})b]_a^s \subseteq \Sigma$. Combining the progressions for $i \in [1, m]$, we obtain $[(\lambda + r_{j+1})b + a, (mk + \lambda + r_{j+1})b]_a^{m(s+1)-1} \subseteq \Sigma$. The last element of the progression is $(mk + \lambda + r_{j+1})b = (mk + \lambda + r_j + r - k)b = (\lambda + r_j)b + qb - kb = (\lambda + r_j)b - (p + s + 2)a$. Since $\lambda + r_j \neq 0$ (as $j \in [1, k'-1]$), Lemma 7b implies that $[(\lambda + r_j)b - (p + s + 2)a, (\lambda + r_j)b]_a^{p+s+2} \subseteq \Sigma$. It follows that for $j \in [1, k'-1]$,

$$\text{if } r_{j+1} < r, \text{ then } [(\lambda + r_{j+1})b + a, (\lambda + r_j)b]_a^{\ell+s} \subseteq \Sigma \text{ for } \lambda \in [0, d-1]. \tag{7}$$

The length is due to the calculation $m(s+1) - 1 + p + s + 2 = m(s+1) + p + 1 + s = \ell + s$.

When $j = k' - 1$, $r_{j+1} = r_{k'} = 0 < r$. By (7), $[\lambda b + a, (\lambda + r_{k'-1})b]_a^{\ell+s} \subseteq \Sigma$. Letting $\lambda = 0$ we obtain $[a, r_{k'-1}b]_a^{\ell+s} \subseteq \Sigma$. In the case $d \geq 2$, for $\lambda \in [1, d-1]$, as $\lambda b \in \Sigma(b^q)$, we have $[\lambda b, (\lambda + r_{k'-1})b]_a^{\ell+s+1} \subseteq \Sigma$. This proves part (b)(ii). If $k' \geq 3$, then $r_{j+1} \neq 0$ for $j \in [1, k'-2]$, so $\lambda + r_{j+1} \in [1, r-1]$ and $(\lambda + r_{j+1})b \in \Sigma(b^q)$. With the result in (7), we have $[(\lambda + r_{j+1})b, (\lambda + r_j)b]_a^{\ell+s+1} \subseteq \Sigma$ for $\lambda \in [0, d-1]$ as desired in part (b)(iii) when $r_{j+1} < r$.

If $r_{j+1} > r$, then $r_{j+1} = r_j + r$. This can happen only when $j \in [1, k'-2]$; in particular, $k' \geq 3$. For $\lambda \in [0, d-1]$, $\lambda + r_{j+1} \in [1, k-1]$, and so $(\lambda + r_{j+1})b \in \Sigma(b^q)$. Observe that $[(\lambda + r_{j+1})b, ((m-1)k + \lambda + r_{j+1})b]_a^{(m-1)(s+1)} \subseteq \Sigma$. This is clear if $m = 1$. If $m \geq 2$, then for $i \in [1, m-1]$, $ik + \lambda + r_{j+1} \in [k, q]$. By Lemma 7a, $[((i-1)k + \lambda + r_{j+1})b + a, (ik + \lambda + r_{j+1})b]_a^s \subseteq \Sigma$. Combining the progressions for $i \in [1, m-1]$ and recalling that $(\lambda + r_{j+1})b \in \Sigma(b^q)$, we reach the conclusion that $[(\lambda + r_{j+1})b, ((m-1)k + \lambda + r_{j+1})b]_a^{(m-1)(s+1)} \subseteq \Sigma$. The last element in the progression is $((m-1)k + \lambda + r_{j+1})b = ((m-1)k + \lambda + r_j + r)b = (\lambda + r_j)b + qb - kb = (\lambda + r_j)b - (p + s + 2)a$. As $\lambda + r_j \neq 0$ ($j \in [1, k'-2]$), by Lemma 7b, $[(\lambda + r_j)b - (p + s + 2)a, (\lambda + r_j)b]_a^{p+s+2} \subseteq \Sigma$. It follows that $[(\lambda + r_{j+1})b, (\lambda + r_j)b]_a^{\ell} \subseteq \Sigma$ for $\lambda \in [0, d-1]$, the length is due to $(m-1)(s+1) + p + s + 2 = m(s+1) + p + 1 = \ell$. This completes the proof of part (b)(iii) in the case $r_{j+1} > r$. □

Proposition 1 is our main tool in the proof of Theorem 2. In one direction, assuming minimality and unsplittability, we use it to derive the order of a and the structure of $G/\langle a \rangle$. In the other direction, given the information on $G/\langle a \rangle$ and the relationship between the parameters of α, we infer minimality and use the proposition to conclude unsplittability.

4. Proof of Theorem 2: (1) Implies (2)

In this section, let α be an admissible and unsplittable minimal zero-sum sequence over G. We will show that α is a 2-thread sequence with sum 0 satisfying conditions (a) and (b) in Theorem 2(2).

By Definition 2 there exists a term $a \in supp(\alpha)$ with multiplicity m_a such that $\alpha = a^{m_a}\beta$, $\beta \neq \varnothing$, and $b - b' = xa$ with $x \in [-m_a, m_a]$ for all terms b and b' of β. Write $u \preccurlyeq v$ for $u, v \in G$ if $v = u + xa$ with $x \in [0, m_a]$, and $u \prec v$ if $u \preccurlyeq v$ and $u \neq v$. Also write $u \sim v$ if $u \preccurlyeq v$ or $v \preccurlyeq u$. Observe that $u \sim v$ if and only if $u - v = xa$ with $x \in [-m_a, m_a]$. Denote $P_a = \Sigma(a^{m_a}) = \{a, 2a, \ldots, m_a a\}$ and $P_a^* = P_a \cup \{0\}$.

Since α is a minimal zero-sum sequence, $a \neq 0$ and $m_a \in (0, \mathrm{ord}(a))$. Henceforth an *a-sum* means a subsequence of $\beta = \alpha\left(a^{m_a}\right)^{-1}$ with sum a. Thus, by definition, an a-sum does not reduce to a single term a; consequently its length is at least 2. The terms in an a-sum are not all equal by Lemma 1. We need the following fact about an unsplittable minimal zero-sum sequence α.

Lemma 9 ([4], Lemma 6.1)**.** *a) For each $b \in supp(\beta)$, there is an a-sum containing b.*

b) Let $\sigma|\beta$ be an a-sum. Suppose that $u \in supp(\sigma)$ and $v \in supp(\beta)$ satisfy $v \prec u$. Then σ contains the entire subsequence $v^{m_v}|\alpha$, i.e., all occurrences of v in α.

By Lemma 9a, β contains an a-sum because $\beta \neq \varnothing$. We distinguish two cases.

4.1. Case 1: $\beta = \alpha\left(a^{m_a}\right)^{-1}$ Is an a-sum

Let $\beta = b_1 \ldots b_k$ with $k \geq 2$. Since $S(\alpha) = 0$ and $S(\beta) = a$, $(m_a + 1)a = 0$. As $m_a \in (0, \mathrm{ord}(a))$, we obtain $\mathrm{ord}(a) = m_a + 1$ and $\Sigma(a^{m_a}) = \langle a\rangle \setminus \{0\}$. By the minimality of α and that $b \sim b'$ for all terms b and b' of β, $\langle a\rangle$ is a proper subgroup of G, and all terms in β belong to the same proper a-coset D. Let b be any term in β, then $\{b, b - a, \ldots, b - m_a a\} = b + \langle a\rangle = D$. Since $supp(\beta) \subseteq D$, each $b_j \in \beta$ can be expressed as $b_j = b - s_j a$ with $s_j \in [0, m_a]$. As β is an a-sum, its terms are not all equal, up to relabeling we may assume $b = b_1 \neq b_k$. Now $S(\beta) = a$ implies $kb = (s_1 + \cdots s_k + 1)a$. So far we have shown that α is a 2-thread sequence with $p = m_a$, $q = 0$, and sum 0.

Note that $q = 0$ implies $r = 0$ and $d = k$. By Lemma 2, $\langle a, b\rangle = G$. Recall $b_1 + \cdots + b_k = a \in \langle a\rangle$ and all terms of β are in the same proper a-coset $b + \langle a\rangle$. Due to minimality of α, no nonempty proper subsequence sum of β is in $\langle a\rangle$. This implies that the partial sums $b_1, \ldots, b_1 + \cdots + b_{k-1}$ are in different proper a-cosets. Hence reducing β mod $\langle a\rangle$ yields a minimal zero-sum sequence $\overline{\beta}$ over the factor group $G/\langle a\rangle$. Condition (a) follows, and so does condition (b) as $q = 0$, $p = m_a$, and $|G| = k(m_a + 1)$.

4.2. Case 2: $\beta = \alpha\,(a^{m_a})^{-1}$ Is Not an a-sum

We need the following intuitively obvious fact, which was present in [4] (Section 6.1, Claim 1.2). For completeness we include a proof adjusted to the current setting.

Claim 2. *There exists a term b of $\beta = \alpha\,(a^{m_a})^{-1}$ such that $b' \preccurlyeq b$ for each $b' \in \beta$.*

Proof. Suppose the claim is false. Then, because $b_i \sim b_j$ for all $b_i \in \beta$, $b_j \in \beta$, we conclude that for each $t \in supp(\beta)$ there exists a $t' \in supp(\beta)$ of the form $t' = t + xa$ with $x \in [1, m_a]$. We call such a t' with x minimal the *successor* of t.

Let $\sigma|\beta$ be an a-sum; such sums exist by Lemma 9a because $\beta \neq \varnothing$. We show that $\sigma = \beta$ contrary to the assumption that β is not an a-sum. Suppose that for some $b \in supp(\beta)$ there is an occurrence of b in α that is not a term of σ. By Lemma 9b, neither are all occurrences of its successor b', all occurrences of the successor b'' of b', and so on. A repetition certainly occurs in the row $b, b', b'', \ldots$. The first repeated element is the initially chosen $b \in supp(\beta)$ since $t \mapsto t'$ is an injection. Thus we obtain a subset $X = \{b, b', b'', \ldots\} \subseteq supp(\beta)$ such that no terms of σ is equal to an element of X. Note that the union of the translates $b + P_a^*, b' + P_a^*, b'' + P_a^*, \ldots$ is an entire a-coset D. On the other hand, $supp(\beta) \subseteq D$ by $b_i \sim b_j$ for all $b_i, b_j \in \beta$. Then the definition of a successor implies $X = supp(\beta)$, leading to the impossible $\sigma = \varnothing$. The stated $\sigma = \beta$ follows, completing the proof. □

Fix a term $b \in \beta$ with the property in Claim 2 and let σ be an a-sum containing b. Such a-sums exist by Lemma 9a. Lemma 9b implies that σ contains all terms of β different from b. Hence $\beta = b^q \sigma$ with $q \geq 1$ as β is not an a-sum. Let $\sigma = b_1 \cdots b_k$ with $b_1 = b$, then $b_j = b - s_j a$ where $s_j \in [0, m_a]$ for all $j \in [1, k]$. Note that $s_1 = 0$. Since σ is an a-sum, $k \geq 2$ and the terms in σ are not all equal. Therefore up to relabeling we may assume $b_1 \neq b_k$. Also $S(\sigma) = a$ implies $kb = (s_1 + \cdots + s_k + 1)a$. So far we have reached the conclusion that $\alpha = a^p b^q b_1 \cdots b_k$ is a 2-thread sequence with sum 0, $p = m_a$, and $q \geq 1$. It remains to show that α satisfies the conditions in Theorem 2(2).

4.2.1. An Identity Related to the Conditions in Theorem 2(2)

Proposition 1 states that for a 2-thread sequence with $q \geq 1$ and sum 0, certain a-progressions are in the sumset of the sequence with any arbitrary term removed. Now with minimality, we infer the structure of $\langle a \rangle$ and prove the following identity, which is related to the conditions in Theorem 2(2):

$$d\mathrm{ord}(a) = k(p+1) + q(s+1). \tag{8}$$

Let us first handle the simpler case $r = 0$. Here $q = mk$, $d = k$, and $k' = 1$. Let t be any term in α. Since α is a minimal zero-sum sequence, the sumset $\Sigma(\alpha t^{-1})$ does not contain 0. On the other hand, by Proposition 1a, $[a, -a]_a^{\ell-2} \subseteq \Sigma(\alpha t^{-1})$, that is,

$-a = a + (\ell - 2)a = (\ell - 1)a$ and $[a, (\ell - 1)a]_a^{\ell-2} \subseteq \Sigma(\alpha t^{-1})$. As the a-progression does not contain 0, we obtain $\ell \le \mathrm{ord}(a)$. Since $-\ell a = rb = 0$ (Lemma 4), it follows that $\ell = \mathrm{ord}(a)$, i.e., $\mathrm{ord}(a) = p+1+m(s+1)$. Multiply the last equation by $d = k$, and we obtain identity (8) in the case $r = 0$.

Suppose $r \neq 0$, then $k' \geq 2$. Lemma 4 implies $r_j b \in \langle a \rangle$ for $j \in [0, k' - 1]$ and suggests a decreasing order of the a-coordinates. The following claim confirms it by using Proposition 1 and the minimality of α.

Claim 3. *Suppose $r \neq 0$. Then $x_a(r_0 b) = \mathrm{ord}(a)$, $x_a(r_1 b) = \mathrm{ord}(a) - \ell$, and $x_a(r_{k'-1} b) = \ell + s + 1$. If $k' \geq 3$, then for $j \in [1, k' - 2]$, $x_a(r_{j+1} b) = x_a(r_j b) - L$, where $L = \ell$ if $r_{j+1} > r$ or $L = \ell + s + 1$ if $r_{j+1} < r$.*

Proof. Let $t \in supp(\alpha)$ and consider $\Sigma = \Sigma(\alpha t^{-1})$. Since α is a minimal zero-sum sequence, Σ does not contain 0.

By definition, $x_a(r_0 b) = x_a(0) = \mathrm{ord}(a)$. By Proposition 1b(i), $[r_1 b, -a]_a^{\ell-1} \subseteq \Sigma$, i.e., $[r_1 b, r_1 b + (\ell - 1)a]_a^{\ell-1} \subseteq \Sigma$. Since the a-progression does not contain 0, we obtain that $x_a(r_1 b) + (\ell - 1) \leq \mathrm{ord}(a) - 1$, i.e., $x_a(r_1 b) + \ell \leq \mathrm{ord}(a)$. Hence $x_a(r_1 b) + \ell \in [1, \mathrm{ord}(a)]$, and $x_a(r_1 b + \ell a) = x_a(r_1 b) + \ell$. On the other hand, $x_a(r_1 b + \ell a) = \mathrm{ord}(a)$ as $r_1 b + \ell a = 0$. It follows that $x_a(r_1 b) = \mathrm{ord}(a) - \ell$.

By Proposition 1b(ii), $[a, r_{k'-1} b]_a^{\ell+s} \subseteq \Sigma$, i.e., $r_{k'-1} b = a + (\ell + s)a = (\ell + s + 1)a$ and $[a, (\ell + s + 1)a]_a^{\ell+s} \subseteq \Sigma$. Since the progression does not contain 0, we conclude that $\ell + s + 1 \in [1, \mathrm{ord}(a))$ and $x_a(r_{k'-1} b) = \ell + s + 1$.

Suppose $k' \geq 3$. For $j \in [1, k' - 2]$, apply Proposition 1b(iii) with $\lambda = 0$. We have $[r_{j+1} b, r_j b]_a^L \subseteq \Sigma$, where $L = \ell$ if $r_{j+1} > r$ or $L = \ell + s + 1$ if $r_{j+1} < r$. This means $r_j b = r_{j+1} b + La$, and the a-progression starting at $r_{j+1} b$ with length L does not contain 0. It follows that $x_a(r_{j+1} b) \in [1, \mathrm{ord}(a))$ and $x_a(r_{j+1} b) + L \in [1, \mathrm{ord}(a))$. Hence $x_a(r_j b) = x_a(r_{j+1} b + La) = x_a(r_{j+1} b) + L$ and $x_a(r_{j+1} b) = x_a(r_j b) - L$. $\square$

Claim 3 implies that $x_a(r_j b)$ is a decreasing sequence for $j \in [0, k' - 1]$. Recall that $r_{k'} = r_0 = 0$. The cyclic group $\langle a \rangle$ can be viewed as partitioned into k' a-progressions starting at $r_{k'} b = 0, r_{k'-1} b, \ldots, r_1 b$. The length of each of the progressions $[r_{j+1} b, r_j b]_a^L$ (for $j \in [0, k' - 1]$) depends on whether r_{j+1} is less than r. More exactly, L is $\ell + s + 1$ if $r_{j+1} < r$ or ℓ if $r_{j+1} \geq r$. Set $r = r'd$. Observe that among $r_1, \cdots, r_{k'-1}, r_{k'}$ exactly r' of them are less than r, since the sequence is a permutation of $0, d, \ldots, (k' - 1)d$ (Remark 2). Therefore

$$\mathrm{ord}(a) = r'(\ell + s + 1) + (k' - r')\ell = r'(s + 1) + k'\ell = k'(p + 1) + (mk' + r')(s + 1).$$

Multiply the above by d, and we obtain identity (8) in the case $r \neq 0$.

4.2.2. Conditions (a) and (b) in Theorem 2(2)

Now we show that α satisfies the conditions in Theorem 2(2). As condition (b) follows from condition (a) and identity (8), it is enough to establish condition (a).

Since α is an unsplittable minimal zero-sum sequence, we have $\langle \alpha \rangle = G$ and hence $\langle a, b \rangle = G$. Recall that $d = \gcd(q, k)$ and $db \in \langle a \rangle$. If $d = 1$ then $G = \langle a \rangle$, so condition (a) in Theorem 2(2) holds with $G/\langle a \rangle$ being the trivial group.

For $d \geq 2$, to prove condition (a), we argue that d is the smallest positive integer such that $db \in \langle a \rangle$. Let t be any term in α. Observe that $\lambda b + \langle a \rangle \subseteq \Sigma(\alpha t^{-1})$ for $\lambda \in [1, d-1]$. This follows from Proposition 1a in the case $r = 0$. Suppose $r \neq 0$. Recall from Section 4.2.1 that the cyclic group $\langle a \rangle$ can be viewed as partitioned into k' a-progressions starting at $r_{k'}b = 0, r_{k'-1}b, \ldots, r_1 b$; denote these progressions by $P_{k'}, P_{k'-1}, \ldots, P_1$. Let $\lambda \in [1, d-1]$. The translates of $P_{k'}, P_{k'-1}, \ldots, P_1$ by λb: $\lambda b + P_{k'}, \lambda b + P_{k'-1}, \ldots, \lambda b + P_1$ form a partition of $\lambda b + \langle a \rangle$, with first elements at $(\lambda + r_{k'})b, (\lambda + r_{k'-1})b, \ldots, (\lambda + r_1)b$. By Proposition 1b, these a-progressions are all in $\Sigma(\alpha t^{-1})$. Hence $\lambda b + \langle a \rangle \subseteq \Sigma(\alpha t^{-1})$. By the minimality of α, $0 \notin \Sigma(\alpha t^{-1})$. Therefore for $\lambda \in [1, d-1]$, $\lambda b + \langle a \rangle \neq \langle a \rangle$, and it follows that $\lambda b \notin \langle a \rangle$. This completes the proof that α satisfies condition (a) of Theorem 2(2).

5. Proof of Theorem 2: (2) Implies (1)

In this section, let $\alpha = a^p b^q b_1 \cdots b_k$ be a 2-thread sequence with sum 0 satisfying the conditions in Theorem 2(2). We will show that α is an admissible and unsplittable minimal zero-sum sequence.

Remark 5. As noted in Remark 1, any 2-thread sequence $\alpha = a^p b^q \sigma$ is admissible, although it is not necessary that $p = m_a$, where m_a is the multiplicity of a in α. With the conditions in Theorem 2(2), we will show that $p = m_a$, i.e., $b_i \neq a$ for $i \in [1, k]$. This is obvious in the case $d \geq 2$ by condition (a) of Theorem 2(2), since $\langle a \rangle$ is a proper subgroup of G and all terms in $b^q \sigma$ belong to a proper a-coset. The case $d = 1$ excludes $q = 0$ and $r = 0$ as then $d = k \geq 2$.

5.1. Case 1: $\alpha = a^p \sigma$ ($q = 0$)

We already know that α is a zero-sum sequence and $p = m_a$ (Remark 5). Conditions (a) and (b) in Theorem 2(2) give $|G| = d\operatorname{ord}(a) = k(p+1)$, and therefore $\operatorname{ord}(a) = p + 1$ ($d = k$). Since α is a 2-thread sequence, all terms of σ belong to the same proper a-coset $b + \langle a \rangle$. As $|\sigma| = k = d$, no nonempty proper subsequence of σ has sum in $\langle a \rangle$ by condition (a). Let $a^x \tau | \alpha$ be a nonempty zero-sum subsequence such that $x \in [0, p]$ and $\tau | \sigma$. Since $S(a^x \tau) = 0 \in \langle a \rangle$, $S(\tau) \in \langle a \rangle$ and hence $\tau \in \{\varnothing, \sigma\}$. It is not possible that $\tau = \varnothing$ as otherwise $1 \leq x \leq p < \operatorname{ord}(a)$ and $a^x \tau$ is not a zero-sum. Therefore $\tau = \sigma$ and $S(a^x \tau) = (x+1)a$. Now $1 \leq x + 1 \leq p + 1$ and $\operatorname{ord}(a) = p + 1$ imply that $x = p$, and hence α is a minimal zero-sum sequence.

It remains to show that α is unsplittable. By Lemma 2, it is enough to show that $\Sigma(\alpha t^{-1}) = G^\bullet$ for each $t \in \mathit{supp}(\alpha)$. In fact checking the inclusion $G^\bullet \subseteq \Sigma(\alpha t^{-1})$

suffices because αt^{-1} is zero-sum-free. First, we show that $G^\bullet \subseteq \Sigma(\alpha b_0^{-1})$ for any $b_0 \in \sigma$. Note that $\alpha b_0^{-1} = a^p(\sigma b_0^{-1})$. Since $\mathrm{ord}(a) = p+1$, $\Sigma(a^p) = \langle a\rangle \setminus \{0\}$. By condition (a), nonempty subsequence sums of σb_0^{-1} with different lengths are in different proper a-cosets; hence the translates of $\Sigma^*(a^p)$ by these subsequence sums as the lengths range over $[1, k-1]$ cover all the $k-1$ proper a-cosets. The conclusion follows. Now we show $G^\bullet \subseteq \Sigma(\alpha a^{-1})$. Note that $\alpha a^{-1} = a^{p-1}\sigma$ and $\Sigma(a^{p-1}) = \langle a\rangle \setminus \{0, -a\}$. As $b_1 \neq b_k$, $(b_1 + \Sigma^*(a^{p-1})) \cup (b_k + \Sigma^*(a^{p-1})) = b + \langle a\rangle$ follows. If $k = 2$, then the unique proper a-coset is covered. If $k \geq 3$, to cover the remaining proper cosets, notice that the nonempty subsequence sums of the remaining terms in $\sigma(b_1 b_k)^{-1}$ with different lengths are in different proper a-cosets; so the translates of $b + \langle a\rangle$ by these subsequence sums as the lengths range over $[1, k-2]$ cover all the remaining proper cosets. Finally, note that $S(\alpha a^{-1}) = -a$, and the conclusion follows.

5.2. Case 2: $\alpha = a^p b^q \sigma$ with $q \geq 1$

5.2.1. Minimality

We first handle the simpler case $r = 0$. Here $d = k$, and $q = mk$ with $m \geq 1$ as $q \geq 1$. We know $p = m_a$ (Remark 5). By conditions (a) and (b) of Theorem 2(2), $k(p+1) + q(s+1) = k\mathrm{ord}(a)$, which gives $\mathrm{ord}(a) = p + 1 + m(s+1)$. Let $\tau = a^t\gamma$ be a nonempty zero-sum subsequence of α, with $t \in [0, p]$ and $\gamma | b^q\sigma$. Clearly $\gamma \neq \varnothing$ as $\mathrm{ord}(a) > p$. Since $S(\gamma) \in \langle a\rangle$, condition (a) of Theorem 2(2) implies that $|\gamma|$ must be a multiple of k. Suppose γ is a proper subsequence of $b^q\sigma$. Then $|\gamma| = x'k$ with $x' \in [1, m]$, as $|b^q\sigma| = (m+1)k$. So $S(\gamma) = x'kb - s'a = x'(s+1)a - s'a$ for some $s' \in [0, s]$. Hence $S(\tau) = ta + S(\gamma) = (t + x'(s+1) - s')a$. Now $t + x'(s+1) - s' \geq s + 1 - s' \geq 1$, and $t + x'(s+1) - s' \leq p + m(s+1) = \mathrm{ord}(a) - 1$ imply that τ cannot be a zero-sum. Therefore $\gamma = b^q\sigma$. Since $S(\alpha) = 0$, $S(\gamma) = -pa$, we have $S(\tau) = ta + S(\gamma) = (t-p)a$, with $-\mathrm{ord}(a) < -p \leq t - p \leq 0$. The only way for τ to be a zero-sum is when $t = p$, and hence $\tau = \alpha$. This proves that α is a minimal zero-sum sequence.

For the remaining of Section 5.2.1 we suppose $r \neq 0$. In this case, $d < k$ and $k' \geq 2$. By Lemma 4, $r_j b \in \langle a\rangle$ for $j \in [1, k'-1]$. In the following lemma, using conditions in Theorem 2(2), we compute the a-coordinates of $r_j b$'s and justify that they are in a decreasing order.

Lemma 10. *Suppose $r \neq 0$. Then:*

a) for $j \in [1, k'-1]$, $x_a(r_j b) = \frac{1}{k}\big(r_j(s+1) + (k - jd)\mathrm{ord}(a)\big)$, and $x_a(r_j b) < \mathrm{ord}(a)$;

b) $x_a(r_j b)$ is a decreasing function of $j \in [1, k'-1]$; more exactly, if $k' \geq 3$, then for $j \in [1, k'-2]$, $x_a(r_j b) - x_a(r_{j+1} b) = L$, where $L = \ell$ if $r_{j+1} > r$ or $L = \ell + s + 1$ if $r_{j+1} < r$.

Proof. a) First we show that for $j \in [1, k'-1]$, $r_j b = \frac{1}{k}\big(r_j(s+1) + (k-jd)\mathrm{ord}(a)\big)a$ by induction on j.

Conditions (a) and (b) of Theorem 2(2) imply that

$$k(p+1) + q(s+1) = d\mathrm{ord}(a), \qquad \text{i.e.,} \qquad k\ell + r(s+1) = d\mathrm{ord}(a). \tag{9}$$

Hence $\ell = \frac{1}{k}\big(d\mathrm{ord}(a) - r(s+1)\big)$. Since $rb = -\ell a$ (Lemma 4) and $r_1 = r$, we have $r_1 b = \big(\mathrm{ord}(a) - \ell\big)a = \frac{1}{k}\big(r_1(s+1) + (k-d)\mathrm{ord}(a)\big)a$, which is the base case $j = 1$.

For the inductive step, suppose the formula holds for $j \in [1, k'-2]$; then

$$r_j b + rb = \frac{1}{k}\big((r_j + r)(s+1) + (k-(j+1)d)\mathrm{ord}(a)\big)a.$$

By Lemma 3, $r_{j+1} = r_j + r$ if $r_{j+1} \geq r$ or $r_{j+1} = r_j + r - k$ if $r_{j+1} < r$. As $kb = (s+1)a$, we have $r_{j+1}b = \frac{1}{k}(r_{j+1}(s+1) + (k-(j+1)d)\mathrm{ord}(a))a$ in either case, and this completes the induction.

Now we show that for $j \in [1, k'-1]$, $0 < \frac{1}{k}\big(r_j(s+1) + (k-jd)\mathrm{ord}(a)\big) < \mathrm{ord}(a)$, and part (a) will follow. Since $j \in [1, k'-1]$, $r_j > 0$, $jd \in [d, k-d]$, and $k - jd > 0$; the lower bound follows. The upper bound is equivalent to $r_j(s+1) - jd\mathrm{ord}(a) < 0$. By (9) it is equivalent to $jk(p+1) + (jq - r_j)(s+1) > 0$, which holds because by definition $r_j \leq jr \leq jq$ and $jk(p+1) > 0$.

b) Suppose $k' \geq 3$. By part (a) and the second identity in (9), we have that for $j \in [1, k'-2]$,

$$x_a(r_j b) - x_a(r_{j+1}b) = \frac{1}{k}\big((r_j - r_{j+1})(s+1) + d\mathrm{ord}(a)\big) = \ell + \frac{1}{k}(r_j - r_{j+1} + r)(s+1).$$

If $r_{j+1} > r$, then $r_j - r_{j+1} = -r$, and $x_a(r_j b) - x_a(r_{j+1}b) = \ell$. If $r_{j+1} < r$, then $r_j - r_{j+1} = -r + k$, and $x_a(r_j b) - x_a(r_{j+1}b) = \ell + s + 1$. $\square$

Remark 6. Lemma 10b implies that

$$\max_{j \in [1, k'-1]} x_a(r_j b) = x_a(r_1 b) \qquad \text{and} \qquad \min_{j \in [1, k'-1]} x_a(r_j b) = x_a(r_{k'-1}b).$$

Recall that $r_{k'-1} = k - r$ (Remark 2). Let $j = k' - 1$ in Lemma 10a, then $x_a(r_{k'-1}b) = \frac{1}{k}\big((k-r)(s+1) + d\mathrm{ord}(a)\big) = \ell + s + 1$ by the second identity in (9). Moreover, $\mathrm{ord}(a) > \ell + s + 1$ as $x_a(r_{k'-1}b) < \mathrm{ord}(a)$. On the other hand, since $r_1 b = \big(\mathrm{ord}(a) - \ell\big)a$ and $0 < \mathrm{ord}(a) - \ell < \mathrm{ord}(a)$, it follows that $x_a(r_1 b) = \mathrm{ord}(a) - \ell$. In summary,

$$\max_{j \in [1, k'-1]} x_a(r_j b) = \mathrm{ord}(a) - \ell \qquad \text{and} \qquad \min_{j \in [1, k'-1]} x_a(r_j b) = \ell + s + 1. \tag{10}$$

We are ready to show that $p = m_a$. By Remark 5 we only need to consider $d = 1$. In this case, $G = \langle a \rangle$ and $k = k'd = k'$. Apply Lemma 10a with $d = 1$, we have $x_a(r_j b) = \frac{1}{k}\big(r_j(s+1) + (k-j)\mathrm{ord}(a)\big)$ for $j \in [1, k-1]$. Let $j_0 \in [1, k-1]$ be such that $r_{j_0} = d = 1$, then $x_a(b) = \frac{1}{k}\big(s + 1 + (k - j_0)\mathrm{ord}(a)\big)$ and $x_a(b) \in (0, \mathrm{ord}(a))$. In fact $x_a(b) \geq p + 2$. Indeed, $j_0 \in [1, k-1]$ implies $k - j_0 \in [1, k-1]$. Let $d = 1$ in the first identity in (9), then $\mathrm{ord}(a) = k(p+1) + q(s+1)$. As $q \geq 0$ and $s \geq 0$,

$$x_a(b) \geq \frac{1}{k}\big((s+1) + \mathrm{ord}(a)\big) = \frac{1}{k}\big(k(p+1) + (q+1)(s+1)\big) > p + 1.$$

Since $x_a(b)$ is an integer, $x_a(b) \geq p + 2$ follows. Recall that in the 2-thread sequence α, for $i \in [1, k]$, $b_i = b - s_i a$ with $s_i \in [0, p]$. As $x_a(b) \in [p + 2, \mathrm{ord}(a))$, we obtain that $b_i = (x_a(b) - s_i)a$ where $x_a(b) - s_i \in [2, \mathrm{ord}(a))$. Hence $b_i \neq a$ for $i \in [1, k]$, and $p = m_a$ follows.

One can further show that $b_i \notin \{a, \ldots, (p+1)a\}$ for $i \in [1, k]$, which is analogous to a condition in Theorem 1(i). This follows once we know that α is an unsplittable minimal zero-sum sequence. It is more interesting that we can prove it directly using an approach similar to the argument above for $b_i \neq a$. The details are omitted.

Now we show the minimality of α in the case $r \neq 0$. Let $\tau = a^t\gamma$ be a nonempty subsequence of $\alpha = a^p b^q \sigma$ with sum 0, where $t \in [0, p]$ and $\gamma | b^q\sigma$. Notice that $\gamma \neq \varnothing$ since $\mathrm{ord}(a) > \ell + s + 1 > p$; and $|\gamma| \leq |b^q\sigma| = q + k = (m+1)k + r$. Write $|\gamma| = xk + y$ with $0 \leq y < k$; clearly $x \in [0, m+1]$ and $x + y > 0$. The sum of γ is $S(\gamma) = |\gamma|b - s'a$, where $s' = \sum_{b_i \in \gamma} s_i$ satisfies $0 \leq s' \leq s$. As $S(\gamma) \in \langle a \rangle$, condition (a) of Theorem 2(2) implies that $|\gamma|$ is a multiple of d. The same is true for k, hence $y \in [0, k)$ is a multiple of d too. Then by Lemma 3a, $y = r_i$ for some $i \in [0, k'-1]$. So $S(\gamma) = |\gamma|b - s'a = xkb + r_i b - s'a = x(s+1)a + r_i b - s'a$.

Let us first reject $i = 0$, that is, $y = r_0 = 0$. In this case $S(\gamma) = Ca$ where $C = x(s+1) - s'$. Note that $C \leq (m+1)(s+1) = (\ell + s + 1) - (p + 1)$. Thus $C < \mathrm{ord}(a) - (p+1)$ (by $\mathrm{ord}(a) > \ell + s + 1$). On the other hand, $C \geq (s+1) - s' \geq 1$ ($y = 0$ implies $x > 0$). Hence $C \in [1, \mathrm{ord}(a) - (p+1))$. This contradicts $S(\tau) = 0$.

Hence $i \in [1, k'-1]$, and $S(\gamma) = Ca$ where $C = x(s+1) + x_a(r_i b) - s'$. Note that $C > 0$ as $x \geq 0$, $s' \leq s$, and $x_a(r_i b) \geq \ell + s + 1$ by the result in (10). Suppose that $x \leq m$. Then since $x_a(r_i b) \leq \mathrm{ord}(a) - \ell$ by (10) and $m(s+1) = \ell - (p+1)$, we have $C \leq \ell - (p+1) + \mathrm{ord}(a) - \ell = \mathrm{ord}(a) - (p+1)$. This contradicts $S(\tau) = 0$. Thus $x = m + 1$, implying $y = r_i \in (0, r]$. We show that $y = r$, i.e., $i = 1$. Otherwise $y = r_i$ with $i \in [2, k'-1]$; in particular $k' \geq 3$. Note $i - 1 \in [1, k'-2]$. Since $r_i < r$, by Lemma 10b, $x_a(r_{i-1}b) - x_a(r_i b) = \ell + s + 1$. As $x_a(r_{i-1}b) < \mathrm{ord}(a)$, we have $x_a(r_i b) = x_a(r_{i-1}b) - (\ell + s + 1) < \mathrm{ord}(a) - (\ell + s + 1)$. It follows that $C = x(s+1) + x_a(r_i b) - s' < (m+1)(s+1) + \mathrm{ord}(a) - (\ell + s + 1) - s'$. We conclude that $C < \mathrm{ord}(a) - (p+1)$, which again contradicts $S(\tau) = 0$.

In summary, $x = m + 1$ and $y = r$, meaning that $\gamma = b^q\sigma$. Since $S(\alpha) = 0$, $S(\gamma) = -pa$. So $S(\tau) = 0$ implies $t = p$ and $\tau = \alpha$, completing the proof of minimality.

5.2.2. Unsplittability

We have shown that α is a minimal zero-sum sequence. To show that it is unsplittable, it is enough to verify $\Sigma(\alpha t^{-1}) = G^\bullet$ for $t \in supp(\alpha)$ (Lemma 2). In fact checking the inclusion $G^\bullet \subseteq \Sigma(\alpha t^{-1})$ suffices because αt^{-1} is zero-sum-free.

By condition (a) of Theorem 2(2), G is the union of cosets $\lambda b + \langle a \rangle$, with $\lambda \in [0, d-1]$. If $r = 0$, then $G^\bullet \subseteq \Sigma(\alpha t^{-1})$ follows from Proposition 1a. If $r \neq 0$, then Lemma 10 and Remark 6 imply that $\langle a \rangle$ is the union of progressions $[r_{j+1}b, r_j b]_a^L$ with $j \in [0, k'-1]$, where $L = \ell$ if $r_{j+1} \geq r$ or $L = \ell + s + 1$ if $r_{j+1} < r$ (Recall $r_0 = r_{k'} = 0$ and $r_1 = r$). Similarly, for $\lambda \in [1, d-1]$ (in the case $d \geq 2$), the coset $\lambda b + \langle a \rangle$ is the union of progressions $[(\lambda + r_{j+1})b, (\lambda + r_j)b]_a^L$ with $j \in [0, k'-1]$, where $L = \ell$ if $r_{j+1} \geq r$ or $L = \ell + s + 1$ if $r_{j+1} < r$. Therefore $G^\bullet \subseteq \Sigma(\alpha t^{-1})$ follows from Proposition 1b.

References

[1] W. Gao, Zero sums in finite cyclic groups, *Integers* **0** (2000), #A12.

[2] W. 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, *Arch. Math. (Basel)* **105 (4)** (2015), 361–370.

[3] J. Peng and F. Sun, On the unsplittable minimal zero-sum sequences over finite cyclic groups of prime order, *Ars Combin.* **130** (2017), 103–118.

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

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

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

[7] P. Yuan and Y. Li, Long unsplittable zero-sum sequences over a finite cyclic group, *Int. J. Number Theory* **12 (4)** (2016), 979–993.

[8] X. Zeng, Y. Li, and P. Yuan, On a conjecture of Lemke and Kleitman, *Acta Arith.* **168 (3)** (2015), 289–299.

[9] X. Zeng, P. Yuan, and Y. Li, On the structure of long unsplittable minimal zero-sum sequences, *Acta Arith.* **176 (2)** (2016), 131–159.

Appendix.

A. Proofs of Lemmas 7 and 8 when $t \in supp(b^q\sigma)$

The proofs of Lemmas 7 and 8 in the case $t \in supp(b^q\sigma)$ are very similar to the arguments when $t = a$: we use Lemma 5 repeatedly, and the following lemma plays the rôle of Lemma 6.

Lemma 11. *Let $\alpha = a^p b^q \sigma$ be a 2-thread sequence over G with sum 0. Let b_0 be an arbitrary term in σ, denote $\tau = \sigma b_0^{-1}$, and let $\gamma | \tau$ be a nonempty subsequence. Then $[S(b^q\gamma), S(\gamma)]_a^{p+1} \subseteq \Sigma(\alpha b_0^{-1}) = \Sigma(a^p b^q \tau)$.*

Proof. Clearly, $S(\gamma) \in \Sigma(\tau)$ and $[S(b^q\gamma), S(b^q\gamma) + pa]_a^p \subseteq \Sigma(a^p b^q \tau)$. The last element in the progression is $S(b^q\gamma) + pa = S(\gamma) + qb + pa = S(\gamma) - a$ as $qb = -(p+1)a$. It follows that $[S(b^q\gamma), S(\gamma)]_a^{p+1} \subseteq \Sigma(a^p b^q \tau) = \Sigma(\alpha b_0^{-1})$. ☐

Suppose $t \in supp(b^q\sigma)$. Notice that we may assume $t \in \sigma$ since there is at least one b in σ by the definition of a 2-thread sequence. In addition to the notations agreed before, we will use the following in both proofs. Let b_0 be an arbitrary term of σ, where $b_0 = b - s_0 a$ with $s_0 \in [0, p]$. Denote $\tau = \sigma b_0^{-1}$, $\beta' = b^q \tau$, and hence $\alpha b_0^{-1} = a^p b^q \tau = a^p \beta'$. Relabel so that $\tau = b'_1 \cdots b'_{k-1}$, where $b'_j = b - s'_j a$ with $s'_j \in [0, p]$. Define $\tau_0 = \varnothing$, $w_0 = 0$; and for $i \in [1, k-1]$, $\tau_i = b'_1 \cdots b'_i$, $w_i = s'_1 + \cdots + s'_i$. In particular, $\tau_{k-1} = \tau$ and $w_{k-1} = s - s_0$.

A.1. Proof of Lemma 7 in the Case $t \in supp(b^q\sigma)$

Proof. In the following, let $t = b_0$ be an arbitrary term of σ, use the notations agreed before, and $\Sigma = \Sigma(\alpha b_0^{-1}) = \Sigma(a^p \beta')$. For $a^p \beta'$ define elementary a-swaps as in Definition 6.

a) Since $R \in [k, q]$, $b^{R-k+1}\tau$ and b^R are nonempty subsequences of β'. Observe that $b^{R-k+1}\tau \xrightarrow{s-s_0} b^R$, as the latter can be obtained from the former by $k-1$ elementary swaps each time replacing a term in τ by a b in $b^q(b^{R-k+1})^{-1}$. By Lemma 5, $P = [S(b^{R-k+1}\tau), S(b^R)]_a^{s-s_0} \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$.

Clearly, $[S(b^{R-k}a), S(b^{R-k}a) + (p-1)a]_a^{p-1} \subseteq \Sigma(a^p b^q)$. Computing the sums, we have $Q = [(R-k)b + a, (R-k)b + pa]_a^{p-1} \subseteq \Sigma$. Notice that the first element of P is $(R-k+1)b + S(\tau) = (R-k)b + b + a - b_0 = (R-k)b + (s_0+1)a$, which is either in Q or immediately after the last element of Q due to $s_0 \in [0, p]$. Hence starting with Q and continuing with P, we obtain that $[(R-k)b + a, Rb]_a^s \subseteq \Sigma$.

b) Notice that $\lambda + r_j \in [1, k-1]$, because $\lambda + r_j \neq 0$, $\lambda \in [0, d-1]$, and $r_j \in [0, k-d]$. Observe that $b^{\lambda + r_j + q - (k-1)}\tau \xrightarrow{I_1} b^q \tau_{\lambda + r_j}$ with $I_1 = s - s_0 - w_{\lambda + r_j}$, as both are nonempty subsequences of β' and the latter can be obtained from the former by $k-1-(\lambda+r_j)$ elementary swaps replacing the terms in $\tau(\tau_{\lambda+r_j})^{-1}$ by b's from

$b^q(b^{\lambda+r_j+q-(k-1)})^{-1}$. We have $[S(b^{\lambda+r_j+q-(k-1)}\tau), S(b^q\tau_{\lambda+r_j})]_a^{I_1} \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$ (Lemma 5). We also know $[S(b^q\tau_{\lambda+r_j}), S(\tau_{\lambda+r_j})]_a^{p+1} \subseteq \Sigma$ (Lemma 11). Therefore $P_1 = [S(b^{\lambda+r_j+q-(k-1)}\tau), S(\tau_{\lambda+r_j})]_a^{I_1+p+1} \subseteq \Sigma$. On the other hand, we have $\tau_{\lambda+r_j} \xrightarrow{w_{\lambda+r_j}} b^{\lambda+r_j}$, as both are nonempty subsequences of β' and the latter can be obtained from the former by elementary swaps replacing the terms in $\tau_{\lambda+r_j}$ by b's from b^q. Hence $P_2 = [S(\tau_{\lambda+r_j}), S(b^{\lambda+r_j})]_a^{w_{\lambda+r_j}} \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$ (Lemma 5). Combining P_1 and P_2, we obtain that $P = [S(b^{\lambda+r_j+q-(k-1)}\tau), S(b^{\lambda+r_j})]_a^{I_2} \subseteq \Sigma$, where $I_2 = I_1 + p + 1 + w_{\lambda+r_j} = p + (s - s_0) + 1$.

Since $\lambda + r_j \in [1, k-1]$ and $q \geq k$, $b^{\lambda+r_j+q-k}|b^q$ is nonempty. Obviously, $Q = [S(b^{\lambda+r_j+q-k}), S(b^{\lambda+r_j+q-k})+pa]_a^p \subseteq \Sigma(a^p\beta')$. Note that the first element of P is $S(b^{\lambda+r_j+q-(k-1)}\tau) = S(b^{\lambda+r_j+q-k}) + b + S(\tau) = S(b^{\lambda+r_j+q-k}) + (s_0+1)a$, which is either in Q or immediately after the last element of Q due to $s_0 \in [0, p]$. Hence starting with Q and continuing with P, we obtain $[S(b^{\lambda+r_j+q-k}), S(b^{\lambda+r_j})]_a^I \subseteq \Sigma$, where $I = (s_0+1) + I_2 = (s_0+1) + p + (s - s_0) + 1 = p + s + 2$. Computation gives the desired $[(\lambda + r_j)b - (p + s + 2)a, (\lambda + r_j)b]_a^{p+s+2} \subseteq \Sigma$. $\square$

A.2. Proof of Lemma 8 in the Case $t \in supp(b^q\sigma)$

Proof. In the following, let $t = b_0$ be an arbitrary term of σ, use the notations agreed before; in particular, $\beta' = b^r\tau$, $\alpha b_0^{-1} = a^p\beta'$, and $\Sigma = \Sigma(\alpha b_0^{-1}) = \Sigma(a^p\beta')$. For $a^p\beta'$ define elementary a-swaps as in Definition 6. Since $S(\alpha) = 0$ and $q = r$, $rb = -(p+1)a$.

a) Clearly, $[r_1b, r_1b + pa]_a^p \subseteq \Sigma(a^p\beta')$. As $r_1b + pa = -a$, we have $[r_1b, -a]_a^p \subseteq \Sigma$.

Suppose $d \geq 2$ and let $\lambda \in [1, d-1]$. In fact $\lambda \in [1, r-1]$ since $r \neq 0$ implies $r \geq d$. Notice that $\tau_\lambda \xrightarrow{w_\lambda} b^\lambda$, as both are nonempty subsequences of β' and the latter can be obtained from the former by elementary swaps replacing terms in τ_λ by b's in b^r. By Lemma 5, $[S(\tau_\lambda), S(b^\lambda)]_a^{w_\lambda} \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$. On the other hand, $[S(b^r\tau_\lambda), S(\tau_\lambda)]_a^{p+1} \subseteq \Sigma$ (Lemma 11). Combining the two progressions, we have $P = [S(b^r\tau_\lambda), S(b^\lambda)]_a^{p+1+w_\lambda} \subseteq \Sigma$. Since $S(b^r\tau_\lambda) = (\lambda + r)b - w_\lambda a$ with $w_\lambda \geq 0$, and $S(b^\lambda) = \lambda b = (\lambda+r)b + (p+1)a$, we see that $(\lambda+r)b$ is in P and $[(\lambda+r_1)b, \lambda b]_a^{p+1} \subseteq \Sigma$ for $\lambda \in [1, d-1]$. Let us state an additional fact that will be used later:

$$[S(b^r\tau_\lambda), (\lambda + r_1)b]_a^{w_\lambda} \subseteq \Sigma, \qquad \text{for } \lambda \in [0, d-1]. \tag{11}$$

Note that (11) follows from the above when $\lambda \in [1, d-1]$, and it holds trivially for $\lambda = 0$ (recall $\tau_0 = \varnothing$ and $w_0 = 0$).

b) Recall $r_{k'} = r_0 = 0$, and for $j \in [1, k'-1]$, $r_j \in [d, k-d]$ and $r_{j+1} \in [0, k-d]$ (Remark 2); hence $\lambda + r_j \in [d, k-1]$ and $\lambda + r_{j+1} \in [0, k-1]$ (as $\lambda \in [0, d-1]$). We prove the following stronger statement.

Claim 4. *For $j \in [1, k'-1]$ and $\lambda \in [0, d-1]$,*

- *if $r_{j+1} > r$, then $[(\lambda+r_{j+1})b - w_{\lambda+r_j}a, (\lambda+r_j)b]_a^L \subseteq \Sigma$ with $L = p+1+w_{\lambda+r_j}$;*

- *if* $r_{j+1} < r$, *then* $[(\lambda + r_{j+1})b + a, (\lambda + r_j)b]_a^{p+s+1} \subseteq \Sigma$.

First, we show that the claim implies part (b). Suppose $\lambda + r_{j+1} \neq 0$. If $r_{j+1} > r$, then $r_{j+1} = r_j + r$. By the claim, $P = [(\lambda + r_{j+1})b - w_{\lambda+r_j} a, (\lambda + r_j)b]_a^L \subseteq \Sigma$, where $L = p + 1 + w_{\lambda+r_j}$. As $w_{\lambda+r_j} \geq 0$ and $(\lambda + r_j)b = (\lambda + r_{j+1})b + (p+1)a$, we have $(\lambda + r_{j+1})b \in P$, and so $[(\lambda + r_{j+1})b, (\lambda + r_j)b]_a^{p+1} \subseteq \Sigma$ as desired. If $r_{j+1} < r$, then since both r_{j+1} and r are multiples of d and $\lambda + r_{j+1} \neq 0$, $\lambda + r_{j+1} \in [1, r-1]$. Hence $b^{\lambda + r_{j+1}}$ is a nonempty subsequence of b^r, so $(\lambda + r_{j+1})b \in \Sigma(b^r)$. Combined with the result from the claim, we obtain $[(\lambda + r_{j+1})b, (\lambda + r_j)b]_a^{p+s+2} \subseteq \Sigma$. Suppose $\lambda + r_{j+1} = 0$, that is $\lambda = 0$ and $j = k' - 1$; as $r_{j+1} = r_{k'} = 0 < r$, $[a, r_{k'-1}b]_a^{p+s+1} \subseteq \Sigma$ follows from the claim.

Before proving the claim, we show by induction on j that for $j \in [1, k'-1]$ and $\lambda \in [0, d-1]$,

$$[S(\tau_{\lambda+r_j}), (\lambda + r_j)b]_a^{w_{\lambda+r_j}} \subseteq \Sigma. \tag{12}$$

For the base case, let $j = 1$ and $\lambda \in [0, d-1]$. Note that we have $r_1 = r$ and $\lambda + r \in [1, k-1]$. Observe that $\tau_{\lambda+r} \xrightarrow{J} b^r \tau_\lambda$ with $J = w_{\lambda+r} - w_\lambda$, as both are nonempty subsequences of β' and the latter can be obtained from the former by r elementary swaps replacing the terms in $\tau_{\lambda+r}(\tau_\lambda)^{-1}$ by b^r. Hence $[S(\tau_{\lambda+r}), S(b^r\tau_\lambda)]_a^J \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$ (Lemma 5). Together with the result in (11), we have $[S(\tau_{\lambda+r_1}), (\lambda + r_1)b]_a^{w_{\lambda+r_1}} \subseteq \Sigma$ as desired.

For the inductive step $j \mapsto j+1$, suppose (12) holds for $j \in [1, k'-2]$. Note that $j + 1 \in [2, k'-1]$, so $r_j, r_{j+1} \in [d, k-d]$, and $\lambda + r_j, \lambda + r_{j+1} \in [1, k-1]$. We need to show that

$$[S(\tau_{\lambda+r_{j+1}}), (\lambda + r_{j+1})b]_a^{w_{\lambda+r_{j+1}}} \subseteq \Sigma. \tag{13}$$

If $r_{j+1} < r$, then $\lambda + r_{j+1} \leq r$ (both r_{j+1} and r are multiples of d). Clearly $\tau_{\lambda+r_{j+1}} \xrightarrow{w_{\lambda+r_{j+1}}} b^{\lambda+r_{j+1}}$, as both are nonempty subsequences of β' and the latter can be obtained by replacing the terms in the former by b's in b^r. Lemma 5 implies $[S(\tau_{\lambda+r_{j+1}}), S(b^{\lambda+r_{j+1}})]_a^{w_{\lambda+r_{j+1}}} \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$, and the desired (13) follows.

If $r_{j+1} > r$, then $r_{j+1} = r_j + r$. We know $[S(\tau_{\lambda+r_j}), (\lambda + r_j)b]_a^{w_{\lambda+r_j}} \subseteq \Sigma$ (inductive hypothesis), and $[S(b^r\tau_{\lambda+r_j}), S(\tau_{\lambda+r_j})]_a^{p+1} \subseteq \Sigma$ (Lemma 11). Hence $Q = [S(b^r\tau_{\lambda+r_j}), (\lambda + r_j)b]_a^{J_1} \subseteq \Sigma$, where $J_1 = p + 1 + w_{\lambda+r_j}$. By computation, $S(b^r\tau_{\lambda+r_j}) = (\lambda + r_{j+1})b - w_{\lambda+r_j}a$ and $(\lambda + r_j)b = (\lambda + r_{j+1})b + (p+1)a$. As $w_{\lambda+r_j} \geq 0$, we have $(\lambda + r_{j+1})b$ is in Q and $Q_1 = [S(b^r\tau_{\lambda+r_j}), (\lambda + r_{j+1})b]_a^{w_{\lambda+r_j}} \subseteq \Sigma$. On the other hand, $\tau_{\lambda+r_{j+1}} \xrightarrow{J_2} b^r\tau_{\lambda+r_j}$ with $J_2 = w_{\lambda+r_{j+1}} - w_{\lambda+r_j}$, as both are nonempty subsequences of β' and the latter can be obtained from the former by r elementary swaps replacing terms in $\tau_{\lambda+r_{j+1}}(\tau_{\lambda+r_j})^{-1}$ by b^r. Hence $Q_2 = [S(\tau_{\lambda+r_{j+1}}), S(b^r\tau_{\lambda+r_j})]_a^{J_2} \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$ (Lemma 5). Combining Q_2 and Q_1, we obtain (13). This completes the induction and the proof of (12)

Finally, we are ready to prove Claim 4. Let $j \in [1, k'-1]$ and $\lambda \in [0, d-1]$. Note that $\lambda + r_j \in [1, k-1]$. We know $[S(b^r\tau_{\lambda+r_j}), S(\tau_{\lambda+r_j})]_a^{p+1} \subseteq \Sigma$ (Lemma 11).

Together with (12), we have

$$[S(b^r\tau_{\lambda+r_j}),(\lambda+r_j)b]_a^{p+1+w_{\lambda+r_j}} \subseteq \Sigma. \tag{14}$$

If $r_{j+1} > r$, then $r_{j+1} = r_j + r$, and we see that (14) is the desired conclusion as $S(b^r\tau_{\lambda+r_j}) = (\lambda + r_{j+1})b - w_{\lambda+r_j}a$. If $r_{j+1} < r$, then $r_{j+1} = r_j + r - k$ and $\lambda + r_{j+1} \in [0, r-1]$. Note that $b^{\lambda+r_{j+1}+1}\tau \xrightarrow{H} b^r\tau_{\lambda+r_j}$, where $H = s - s_0 - w_{\lambda+r_j}$, as both are nonempty subsequences of β' and the latter can be obtained from the former by $k - 1 - (\lambda + r_j)$ elementary swaps, each time replacing a term in $\tau(\tau_{\lambda+r_j})^{-1}$ by a b in $b^r(b^{\lambda+r_{j+1}+1})^{-1}$. Hence $P_1 = [S(b^{\lambda+r_{j+1}+1}\tau), S(b^r\tau_{\lambda+r_j})]_a^H \subseteq \Sigma(a^{p-1}\beta') \subseteq \Sigma$ (Lemma 5). On the other hand, since $\lambda + r_{j+1} \in [0, r-1]$, we have $P_2 = [(\lambda + r_{j+1})b + a, (\lambda + r_{j+1})b + pa]_a^{p-1} \subseteq \Sigma(a^pb^r)$. Observe that the first element of P_1 is $S(b^{\lambda+r_{j+1}+1}\tau)=(\lambda + r_{j+1})b + b + S(\tau) = (\lambda + r_{j+1})b + (s_0 + 1)a$, which is either in P_2 or immediately after the last element of P_2 due to the fact that $s_0 \in [0, p]$. Therefore starting with P_2 and continuing with P_1, we obtain that the a-progression $[(\lambda + r_{j+1})b + a, S(b^r\tau_{\lambda+r_j})]_a^{s-w_{\lambda+r_j}} \subseteq \Sigma$. Together with (14), we reach the desired conclusion $[(\lambda + r_{j+1})b + a, (\lambda + r_j)b]_a^{p+s+1} \subseteq \Sigma$. This completes the proof of Claim 4 and the lemma. □