THE GAP PARTITION LAW IN ADDITION CHAINS

THEOPHILUS AGAMA

Abstract. We prove that the spacing between consecutive terms in an addition chain with non-decreasing τ-track can be generated by adding two previous terms in the chain.

1. Introduction

Let $s_o = 1, s_1 = 2, \ldots, s_h = n$ be an addition chain leading to n with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ such that $i > \sigma(i) \geq \tau(i)$ for each $1 \leq i \leq h$. We say that a chain is a *closed* addition chain if for each $1 \leq i \leq h$ there exists some $j \in [0, h]$ such that

$$s_i - s_{i-1} = s_j$$

and for $s_{\sigma(i)} - s_{\sigma(i-1)} \neq 0$ there exists some $j \in [0, h]$ such that

$$s_{\sigma(i)} - s_{\sigma(i-1)} = s_j.$$

Additionally, for each $s_j = s_{\tau(i)}$ with $s_{\tau(i)} \neq s_{\sigma(k)}$ for all $k \in [0, h]$ there exist some $s_{\sigma(k)}$ such that $s_{\sigma(k)} < s_{\tau(i)}$ is consecutive.
We call a number for which a *closed* addition chain is optimal a *complete* number. In [1], it has been shown that the numbers for which closed addition chains are optimal (complete numbers) satisfy the inequality

$$\ell(2^n - 1) \leq n - 1 + \ell(n)$$

where $\ell(\cdot)$ denotes the length of an optimal addition chain leading to $\cdot$. In [1], we conjectured

Conjecture 1.1. *Let $s_o = 1, s_1 = 2, \ldots, s_h = n$ be an optimal addition chain leading to n with $h := \iota(n)$ such that $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for $i > \sigma(i) \geq \tau(i) \geq 0$ for $1 \leq i \leq h$. Then for each $1 \leq i \leq h$ with $s_{\sigma(i)} - s_{\sigma(i-1)} \neq 0$, there exists some $j \in [0, h]$ such that*

$$s_{\sigma(i)} - s_{\sigma(i-1)} = s_j.$$

In general, all optimal addition chains are closed.

Date: July 4, 2025.
Key words and phrases. Gap.

In the spirit of conjecture 1.1, we prove the gap partition law, an assertion that the gap between consecutive terms in addition chains with a non-decreasing τ-track must be a term in the chain or expressible as a sum of two terms in the chain.

2. Main result

Theorem 2.1 (The gap partition law). *Let*

$$E(n) : s_o = 1, s_1 = 2, \ldots, s_h = n$$

be an addition chain leading to n. Write $s_i = s_{\sigma(i)} + s_{\tau(i)}$ such that $s_{\sigma(i)} \geq s_{\tau(i)} \geq 0$. Define

$$\Delta_i := s_i - s_{i-1}$$

Furthermore, assume that $s_{\tau(i)} \leq s_{\tau(i+1)}$ for each $1 \leq i \leq h-1$. Then there exists $j \geq k$ such that with $s_i \neq 2s_{i-1}$, we have the form

$$\Delta_i = s_j + s_k.$$

Else $\Delta_i \in E(n)$.

Proof. We argue by induction on addition chains. Consider an addition chain leading to 3 of the form $s_o = 1, s_1 = 2, s_2 = 3$. It is clear that $\Delta_i \in \{s_o, s_1, s_2\}$ for each $1 \leq i \leq 2$. Similarly, consider an addition chain leading to 4 of the form $s_o = 1, s_1 = 2, s_2 = 4$. Here, it is also clear that $\Delta_i \in \{s_o, s_1, s_2\}$ for each $1 \leq i \leq 2$. The claim therefore holds for the base case. Let us assume that the claim is true for a fixed index i with $1 < i < h$. Then we can write

$$\Delta_i = s_j + s_k$$

for $s_j, s_k \in E(n)$. Now, we consider $\Delta_i = s_{i+1} - s_i$. We may assume that $s_{i+1} \neq 2s_i$, since in that case we have trivially $\Delta_i = s_i \in E(n)$. We now write

$$s_{i+1} = s_{\sigma(i+1)} + s_{\tau(i+1)} \quad \text{and} \quad s_i = s_{\sigma(i)} + s_{\tau(i)}$$

for $\sigma(i+1), \tau(i+1) \in [0, i]$ and $\sigma(i), \tau(i) \in [0, i-1]$ with $\tau(i+1) \leq \sigma(i+1)$ and $\tau(i) \leq \sigma(i)$. We can write

$$\Delta_{i+1} = (s_{\sigma(i+1)} - s_{\sigma(i)}) + (s_{\tau(i+1)} - s_{\tau(i)}).$$

We may assume that $s_i \neq s_{\sigma(i+1)}$, because in the case $s_i = s_{\sigma(i+1)}$, we will have

$$\Delta_{i+1} = s_{\tau(i+1)} \in E(n)$$

or that the gap Δ_{i+1} is the sum of two previous terms in the chain $E(n)$ in the case $s_{\tau(i+1)} \neq 1$. We observe that $s_{\sigma(i)} \leq s_{\sigma(i+1)}$ is consecutive provided that $2s_{\sigma(i)} \neq s_{\sigma(i+1)}$. If $s_{\sigma(i)} \leq s_{\sigma(i+1)}$ is consecutive, then $s_{\tau(i)} \leq s_{\tau(i+1)}$ is consecutive provided

$$2s_{\sigma(i)} \neq s_{\sigma(i+1)} \quad \text{or} \quad 2s_{\tau(i)} \neq s_{\tau(i+1)}.$$

To justify the first part of our assertion, suppose that $s_{\sigma(i)} \leq s_{\sigma(i+1)}$ is consecutive with $2s_{\sigma(i)} = s_{\sigma(i+1)}$. We may therefore assume that $s_{\sigma(i)} < s_{\sigma(i+1)}$ since with $s_{\sigma(i)} = s_{\sigma(i+1)}$, we get

$$s_{\sigma(i)} = s_{\sigma(i+1)} = 2s_{\sigma(i)}$$

which is absurd. Now, we write

$$s_{\sigma(i)} < s_{\sigma(i)} + s_{\tau(i)} < s_{\sigma(i)} + s_{\sigma(i)} = s_{\sigma(i+1)}$$

since $s_i \neq s_{\sigma(i+1)}$. It implies that

$$s_{\sigma(i)} < s_i < s_{\sigma(i+1)}$$

violating the assumption that $s_{\sigma(i)} \leq s_{\sigma(i+1)}$ is consecutive. We now justify the second assertion. Suppose $s_{\tau(i)} \leq s_{\tau(i+1)}$ is consecutive with $2s_{\tau(i)} = s_{\tau(i+1)}$ and $2s_{\sigma(i)} = s_{\sigma(i+1)}$. We may assume that $s_{\tau(i)} < s_{\tau(i+1)}$, since with $s_{\tau(i)} = s_{\tau(i+1)}$, we get

$$s_{\tau(i)} = s_{\tau(i+1)} = 2s_{\tau(i)}.$$

We may also assume that $s_{\tau(i)} \neq s_{\sigma(i)}$; otherwise, we obtain

$$s_i = s_{\tau(i)} + s_{\sigma(i)} = 2s_{\tau(i)} = s_{\tau(i+1)}.$$

Since we have assumed that $s_i \neq s_{\sigma(i+1)}$, it implies that for $s_{i+1} := s_{\sigma(i+1)} + s_{\tau(i+1)}$, we have

$$s_{\sigma(i+1)} < s_i = s_{\tau(i+1)}$$

violating the inequality $s_{\tau(i+1)} \leq s_{\sigma(i+1)}$. Furthermore, the inequality

$$s_{\sigma(i)} < 2s_{\tau(i)}$$

must hold. If we suppose the contrary that $s_{\sigma(i)} \geq 2s_{\tau(i)}$, then

$$s_{\tau(i)} \leq \frac{1}{2}s_{\sigma(i)} \implies s_{\sigma(i)} + s_{\tau(i)} \leq \frac{3}{2}s_{\sigma(i)}.$$

Thus, we deduce

$$s_{\sigma(i)} < s_i := s_{\sigma(i)} + s_{\tau(i)} \leq \frac{3}{2}s_{\sigma(i)} < 2s_{\sigma(i)} = s_{\sigma(i+1)}$$

violating the requirement that $s_{\sigma(i)} \leq s_{\sigma(i+1)}$ is consecutive. Piecing this information together, we obtain the inequality

$$s_{\tau(i)} < s_{\sigma(i)} < 2s_{\tau(i)} = s_{\tau(i+1)}$$

contradicting the claim that $s_{\tau(i)} \leq s_{\tau(i+1)}$ is consecutive with $2s_{\tau(i)} = s_{\tau(i+1)}$ and $2s_{\sigma(i)} = s_{\sigma(i+1)}$. This proves the observation. We now complete the induction argument on the addition chain. In the case $s_{\sigma(i+1)} = 2s_{\sigma(i)}$ and $s_{\tau(i+1)} = 2s_{\tau(i)}$, we can simply write

$$\Delta_{i+1} = s_{\sigma(i)} + s_{\tau(i)}$$

and the claim is valid since $s_{\sigma(i)}, s_{\tau(i)} \in E(n)$. In the case $s_{\sigma(i+1)} = 2s_{\sigma(i)}$ and $s_{\tau(i+1)} \neq 2s_{\tau(i)}$, then $s_{\tau(i)} \leq s_{\tau(i+1)}$ must be consecutive. By the inductive hypothesis, there exists some $k \geq 0$ such that

$$s_{\tau(i+1)} - s_{\tau(i)} = s_k \in E(n)$$

and we can write for the gap

$$\Delta_{i+1} = s_{\sigma(i)} + s_k$$

in this case. Else, $\Delta_{i+1} = s_{\sigma(i)} \in E(n)$. In the case $2s_{\sigma(i)} \neq s_{\sigma(i+1)}$ and $2s_{\tau(i)} = s_{\tau(i+1)}$, then necessarily $s_{\sigma(i)} \leq s_{\sigma(i+1)}$ must be consecutive. By the inductive hypothesis, there exists some $j \geq 0$ such that

$$s_{\sigma(i+1)} - s_{\sigma(i)} = s_j \in E(n)$$

and we can write for the gap

$$\Delta_{i+1} = s_j + s_{\tau(i)}$$

in this case. Else, $\Delta_{i+1} = s_{\tau(i)} \in E(n)$. Finally, in the case

$$2s_{\sigma(i)} \neq s_{\sigma(i+1)} \quad \text{and} \quad 2s_{\tau(i)} \neq s_{\tau(i+1)}$$

then $s_{\sigma(i)} \leq s_{\sigma(i+1)}$ and $s_{\tau(i)} \leq s_{\tau(i+1)}$ are consecutive. By the inductive hypothesis, there exist some $j, k \geq 0$ such that

$$s_{\sigma(i+1)} - s_{\sigma(i)} = s_j \quad \text{and} \quad s_{\tau(i+1)} - s_{\tau(i)} = s_k$$

and we can write for the gap

$$\Delta_{i+1} = s_j + s_k$$

in this case. This completes the inductive proof that the gap between consecutive terms in an addition chain can be written as a sum of two previous terms in the chain or Else, it must itself be a term in the chain. □

3. Illustrative examples of the Gap-Partition Law

Below are some examples showing how each non-trivial gap $\Delta_i > 1$ splits as a sum of two previous terms in the chain.

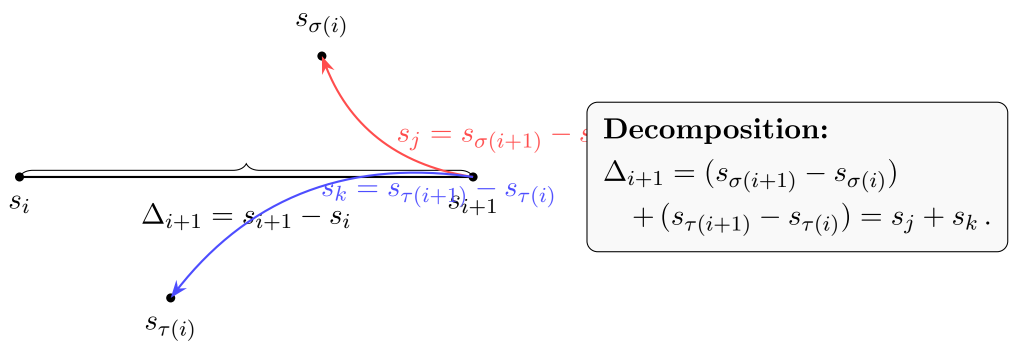

FIGURE 1. Splitting the new gap $\Delta_{i+1} = s_{i+1} - s_i$ into two arcs. The **red** arc peels off the σ-track gap s_j, the **blue** arc the τ-track gap s_k, and the curly brace marks the full gap.

TABLE 1. $n = 12$, chain $1, 2, 4, 8, 12$

i	s_i	$\Delta_i = s_i - s_{i-1}$	Decomposition $\Delta_i = s_j + s_k$
1	2	1	(trivial)
2	4	2	$1 + 1 = s_o + s_o$
3	8	4	$2 + 2 = s_1 + s_1$
4	12	4	$2 + 2 = s_1 + s_1$

TABLE 2. $n = 15$, chain $1, 2, 3, 5, 10, 15$

i	s_i	Δ_i	Decomposition $\Delta_i = s_j + s_k$
1	2	1	(trivial)
2	3	1	(trivial)
3	5	2	$1 + 1 = s_o + s_o$
4	10	5	$3 + 2 = s_2 + s_1$
5	15	5	$3 + 2 = s_2 + s_1$

REFERENCES

1. T. Agama *A note on closed addition chains and complete numbers*, Cryptology ePrint Archive, 2025.

DEPARTEMENT DE MATHEMATIQUES ET DE STATISTIQUE, UNIVERSITE LAVAL, QUEBEC, CANADA.

E-mail address: `thaga1@ulaval.ca/Theophilus@aims.edu.gh/emperordagama@yahoo.com`