ON THE GAP BETWEEN TERMS IN AN ADDITION CHAIN

THEOPHILUS AGAMA

ABSTRACT. In this paper, we study the distribution of the *gap* between terms in an addition chain. In particular, we show that if $1, 2, \dots, s_{\delta(n)} = n$ is an addition chain of length $\delta(n)$ leading to n, then

$$\sup_{1 \leq l \leq \delta(n)} (s_{l+k} - s_l) \gg k \frac{n}{\delta(n)}$$

and

$$\inf_{1 \leq l \leq \delta(n)} (s_{l+k} - s_l) \ll k \frac{n}{\delta(n)}$$

for fixed $k \geq 1$.

1. **Introduction**

The notion of an addition chain producing $n \geq 3$, introduced by Arnold Scholz, is a sequence of numbers of the form

$$1, 2, \dots, s_{k-1}, s_k = n$$

where each term in the sequence is generated by adding two earlier terms and with repetition allowed. Formally each term in the addition chain is of the form $s_k = s_i + s_j$ $(s_k > 1)$ with $i \leq j < k$, and the number of terms in the sequence (excluding 1) is the length of the chain. The length of the smallest such chain producing n is the shortest length of the addition chain. It is a well-known problem to determine the length of the shortest addition chain producing numbers $2^n - 1$ of special forms. A well-known conjecture on the subject, due to Arnold Scholz, purports:

Conjecture 1.1. Let $\iota(n)$ for $n \geq 3$ denote the length of the shortest addition chain producing n, then the inequality

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

holds for all $n \geq 2$.

The conjecture was studied fairly soon after it was published by Alfred Brauer when, who obtained some weaker bounds [1]. There had also been amazing computational work to verify the conjecture [2].

Addition chain is a classic concept in number theory that plays a crucial role in various areas of computational mathematics, including algorithmic number theory, cryptography, and combinatorics. The study of addition chains has deep implications in the efficiency of algorithms that require repeated summations or the

Date: January 13, 2025.

2010 *Mathematics Subject Classification.* Primary 11P81; Secondary 11P82.

Key words and phrases. additive chain; determiners; regulators; length; generators; partition.

representation of numbers through elementary operations, such as those encountered in the computation of exponentiations or the efficient generation of large prime numbers.

Despite their fundamental nature, addition chains are known for their complexity and subtlety, particularly in their asymptotic properties. The length of an addition chain, denoted by $\delta(n)$, has been extensively studied, researchers trying to understand the upper and lower bounds of $\delta(n)$ and to determine the most efficient chains for large n.

In this work, we study the distribution of the gaps between terms in an addition chain. Specifically, we obtain bounds for the largest and smallest gap that can occur between terms, providing information on their asymptotic behavior as a function of n and the length of the chain $\delta(n)$. Our main results established that for fixed $k \geq 1$,

$$\sup_{1\leq l\leq \delta(n)}(s_{l+k}-s_l) \gg k\frac{n}{\delta(n)}$$

and

$$\inf_{1\leq l\leq \delta(n)}(s_{l+k}-s_l) \ll k\frac{n}{\delta(n)}.$$

2. **The regulators and determiners of an addition chain**

In this section, we recall the notion of an addition chain and introduce the notion of the generators of the chain and their accompanying *determiners* and *regulators*.

Definition 2.1. Let $n \geq 3$, then by an addition chain of length $k-1$ producing n, we mean the sequence

$$1, 2, \ldots, s_{k-1}, s_k$$

where each term s_j $(j \geq 3)$ in the sequence is the sum of two earlier terms i.e $s_k = s_i + s_j$ $(s_k > 1)$ with $i \leq j < k$, with the corresponding sequence of partition

$$2 = 1+1, \ldots, s_{k-1} = a_{k-1} + r_{k-1}, s_k = a_k + r_k = n$$

where $a_{i+1} = a_i + r_i$ and $a_{i+1} = s_i$ for $2 \leq i \leq k$. We call the partition $a_i + r_i$ the i^{th} **generator** of the chain for $2 \leq i \leq k$. We call a_i the **determiner** and r_i the **regulator** of the i^{th} generator of the chain. We call the sequence (r_i) the regulators of the addition chain and (a_i) the determiners of the chain for $2 \leq i \leq k$. We call the subsequence (s_{j_m}) for $2 \leq j \leq k$ and $1 \leq m \leq t \leq k$ a truncated addition chain producing n.

At any rate, we do not expect the regulators to be a part of the chain, although the determiners must be the terms in the chain.

Lemma 2.2. *Let* $1, 2, \ldots, s_{k-1}, s_k$ *be an addition chain producing* $n \geq 3$ *with associated generators*

$$2 = 1+1, \ldots, s_{k-1} = a_{k-1} + r_{k-1}, s_k = a_k + r_k = n.$$

Then the following relation for the regulators

$$\sum_{j=2}^{k} r_j = n-1$$

hold.

Proof. We notice that $r_k = n - a_k$. It follows that

$$\begin{aligned} r_k + r_{k-1} &= n - a_k + r_{k-1} \\ &= n - (a_{k-1} + r_{k-1}) + r_{k-1} \\ &= n - a_{k-1}. \end{aligned}$$

Again we obtain from the following iteration

$$\begin{aligned} r_k + r_{k-1} + r_{k-2} &= n - a_{k-1} + r_{k-2} \\ &= n - (a_{k-2} + r_{k-2}) + r_{k-2} \\ &= n - a_{k-2}. \end{aligned}$$

By iterating downwards in this manner the relation follows. □

Corollary 2.1. Let $n \geq 2$ be fixed positive integer and let $1, 2, \ldots, s_{\delta(n)-1}, s_{\delta(n)} = n$ be an addition chain producing n and of length $\delta(n)$, with associated sequence of generators

$$1 + 1, s_2 = a_2 + r_2, \ldots, s_{\delta(n)-1} = a_{\delta(n)-1} + r_{\delta(n)-1}, s_{\delta(n)} = a_{\delta(n)} + r_{\delta(n)} = n$$

then

$$\min\{r_l\}_{l=1}^{\delta(n)} \ll \frac{n}{\delta(n)} \text{ and } \max\{r_l\}_{l=1}^{\delta(n)} \gg \frac{n}{\delta(n)}.$$

We now launch a result which turns out to be useful for constructing the shortest addition chain. In current studies, it has been observed that the *regulators* play a major role in deciding subsequent terms in an addition chain. The following result gives a measure of the scale of our choice of *regulators*. Precisely, it puts a lower and an upper threshold on the magnitude of the choice of regulators for the generators of the shortest addition chain leading to a fixed number $n \geq 2$.

Theorem 2.3. *Let $n \geq 2$ be fixed positive integer and let $1, 2, \ldots, s_{\iota(n)-1}, s_{\iota(n)} = n$ be the shortest addition chain producing n and of length $\iota(n)$, with associated sequence of generators*

$$1 + 1, s_2 = a_2 + r_2, \ldots, s_{\iota(n)-1} = a_{\iota(n)-1} + r_{\iota(n)-1}, s_{\iota(n)} = a_{\iota(n)} + r_{\iota(n)} = n$$

then

$$\min\{r_l\}_{l=1}^{\iota(n)} \ll \frac{n}{\log n} \text{ and } \max\{r_l\}_{l=1}^{\iota(n)} \gg \frac{n}{\log n}.$$

In particular, the magnitude of the regulators in the generator of the shortest addition chain producing n must satisfy $\asymp \frac{n}{\log n}$ as $n \longrightarrow \infty$.

Proof. The claim follows using the fact that the length $\iota(n)$ of the shortest addition chain leading to n satisfies $\iota(n) \asymp \log n$. □

Theorem 2.3 is crucial both in theoretical analysis and for computational purposes because it provides precise bounds for the size of the regulators of the generators of an addition chain. These bounds - characterized by their dependence on the length of the chain and the magnitude n offer key insights into the structure of addition chains, which is fundamental to their efficient construction and analysis.

From a theoretical point of view, the theorem establishes that the minimum and maximum scale of the regulators of an addition chain are on the order of $\frac{n}{\delta(n)}$. This result rigorously quantifies the regularity and variability within the addition chains and ensures that the magnitude of the regulators cannot deviate significantly from this scale.

On the computational side, these results have direct implications for the construction of addition chains. The bound on the regulators guarantees that efficient addition chains can be systematically constructed without using "large" regulators for each generator, which could otherwise increase computational costs. Furthermore, the bounds provide a way to assess the optimality of a given addition chain.

Theorem 2.4. *Let $n \geq 2$ be fixed positive integer and let $1, 2, \ldots, s_{\delta(n)-1}, s_{\delta(n)} = n$ be an addition chain producing n and of length $\delta(n)$, with associated sequence of generators*

$$1+1, s_2 = a_2 + r_2, \ldots, s_{\delta(n)-1} = a_{\delta(n)-1} + r_{\delta(n)-1}, s_{\delta(n)} = a_{\delta(n)} + r_{\delta(n)} = n$$

then

$$\min_{1 \leq l \leq \delta(n)} (s_{l+1} - s_l) \ll \frac{n}{\delta(n)} \text{ and } \max_{1 \leq l \leq \delta(n)} (s_{l+1} - s_l) \gg \frac{n}{\delta(n)}.$$

Proof. Let $n \geq 2$ be a fixed positive integer and consider an addition chain $1, 2, \ldots, s_{\delta(n)-1}, s_{\delta(n)} = n$ producing n and of length $\delta(n)$, with associated sequence of generators

$$1+1, s_2 = a_2 + r_2, \ldots, s_{\delta(n)-1} = a_{\delta(n)-1} + r_{\delta(n)-1}, s_{\delta(n)} = a_{\delta(n)} + r_{\delta(n)} = n$$

and put (a_j) and (r_j) to be the sequence of determiners and regulators, respectively, in the chain. We make the following observations: $s_{\delta(n)-1} = a_{\delta(n)} = a_{\delta(n)-1} + r_{\delta(n)-1} = s_{\delta(n)-2} + r_{\delta(n)-1} = a_{\delta(n)-2} + r_{\delta(n)-2} + r_{\delta(n)-1} = \cdots = 1 + \sum\limits_{j=1}^{\delta(n)-1} r_j = n + 1 - r_{\delta(n)}$, where we have used Lemma 2.2. Similarly, we can write $a_{\delta(n)-1} = 1 + \sum\limits_{j=1}^{\delta(n)-2} = n+1-r_{\delta(n)}-r_{\delta(n)-1}$. Thus by induction, we can write $a_l = n+1-\sum\limits_{j=l}^{\delta(n)} r_j$ for each $3 \leq l \leq \delta(n)$. We observe that $s_{l+1} - s_l = a_{l+2} - a_{i+1} = \sum\limits_{i=l+1}^{\delta(n)} r_i - \sum\limits_{i=l+2}^{\delta(n)} r_i = r_{l+1}$. By corollary 2.1, we deduce that

$$\min_{1 \leq l \leq \delta(n)} (s_{l+1} - s_l) = \min\{r_{l+1}\}_{l=1}^{\delta(n)} \ll \frac{n}{\delta(n)}$$

and

$$\max_{1 \leq l \leq \delta(n)} (s_{l+1} - s_l) = \max\{r_{l+1}\}_{l=1}^{\delta(n)} \gg \frac{n}{\delta(n)}.$$

□

We now extend Theorem 2.4 concerning the gap between consecutive terms in an addition chain to the gap between terms in the chain that are not necessarily consecutive.

Theorem 2.5. *Let $n \geq 2$ be fixed positive integer and let $1, 2, \ldots, s_{\delta(n)-1}, s_{\delta(n)} = n$ be an addition chain producing n and of length $\delta(n)$, with associated sequence of generators*

$$1+1, s_2 = a_2 + r_2, \ldots, s_{\delta(n)-1} = a_{\delta(n)-1} + r_{\delta(n)-1}, s_{\delta(n)} = a_{\delta(n)} + r_{\delta(n)} = n$$

then

$$\sup_{1\leq l\leq \delta(n)}(s_{l+k}-s_{l}) \gg k\frac{n}{\delta(n)}$$

and

$$\inf_{1\leq l\leq \delta(n)}(s_{l+k}-s_{l}) \ll k\frac{n}{\delta(n)}$$

for fixed $k\geq 1$.

Proof. Let $n\geq 2$ be a fixed positive integer and consider an addition chain $1,2,\ldots,s_{\delta(n)-1},s_{\delta(n)}=n$ producing n and of length $\delta(n)$, with associated sequence of generators

$$1+1, s_2=a_2+r_2,\ldots,s_{\delta(n)-1}=a_{\delta(n)-1}+r_{\delta(n)-1}, s_{\delta(n)}=a_{\delta(n)}+r_{\delta(n)}=n$$

and put (a_j) and (r_j) to be the sequence of determiners and regulators, respectively, in the chain. We make the following observations: $s_{\delta(n)-1}=a_{\delta(n)}=a_{\delta(n)-1}+r_{\delta(n)-1}=s_{\delta(n)-2}+r_{\delta(n)-1}=a_{\delta(n)-2}+r_{\delta(n)-2}+r_{\delta(n)-1}=\cdots=1+\sum\limits_{j=1}^{\delta(n)-1}r_j=n+1-r_{\delta(n)}$, where we have used Lemma 2.2. Similarly, we can write $a_{\delta(n)-1}=1+\sum\limits_{j=1}^{\delta(n)-2}=n+1-r_{\delta(n)}-r_{\delta(n)-1}$. Thus by induction, we can write $a_l=n+1-\sum\limits_{j=l}^{\delta(n)}r_j$ for each $3\leq l\leq \delta(n)$. We observe that $s_{l+k}-s_l=a_{l+k+1}-a_{i+1}=\sum\limits_{i=l+1}^{\delta(n)}r_i-\sum\limits_{i=l+k+1}^{\delta(n)}r_i=\sum\limits_{i=l+1}^{l+k}r_i$. It follows that $s_{l+k}-s_l\geq k\ \min\{r_i\}_{i=1+1}^{l+k}$. By corollary 2.1, we deduce that

$$\sup_{1\leq l\leq \delta(n)}(s_{l+k}-s_l)\geq k\sup_{1\leq l\leq \delta(n)}\min\{r_i\}_{i=1+1}^{l+k}\gg k\frac{n}{\delta(n)}.$$

Similarly, we deduce that $s_{l+k}-s_l\leq k\ \max\{r_i\}_{i=l+1}^{l+k}$ and by Corollary 2.1 we get

$$\inf_{1\leq l\leq \delta(n)}(s_{l+k}-s_l)\leq k\inf_{1\leq l\leq \delta(n)}\max\{r_i\}_{i=1+1}^{l+k}\ll k\frac{n}{\delta(n)}$$

thereby ending the proof. □

Utility of Results in Cryptography

The study of gaps between terms in an addition chain, $s_{l+1}-s_l$, has profound implications for both the efficiency and security of cryptographic algorithms. Addition chains are critical for minimizing the computational cost of modular exponentiation, $g^x \mod p$, and scalar multiplication in elliptic curve cryptography (ECC), kP. These operations are foundational to protocols such as RSA, Diffie-Hellman, and ECC-based schemes.

Efficiency in Cryptographic Computations. Theoretical bounds on $s_{l+1}-s_l$ directly inform the construction of addition chains with optimal efficiency. Smaller, controlled gaps reduce the number of squaring and multiplication operations, leading to faster modular exponentiation and scalar multiplication. For instance, in RSA key generation, efficient exponentiation can significantly reduce runtime for large key sizes, improving overall performance.

Side-Channel Attack Resistance. Irregular or randomized gaps disrupt side-channel attack vectors, such as timing and power analysis, which exploit predictable computation patterns. By characterizing and bounding these gaps, our results enable the design of addition chains that balance computational efficiency with obfuscation, adding an additional layer of security to cryptographic implementations.

Broader Implications. Our findings provide a theoretical framework for analyzing and optimizing addition chains under practical cryptographic constraints. This contributes to both the design of efficient cryptographic algorithms and the development of secure implementations resistant to side-channel attacks.

[1].

References

1. A. Brauer, *On addition chains*, Bulletin of the American mathematical Society, vol. 45:10, 1939, 736–739.
2. M. Clift, *Calculating optimal addition chains*, Computing, vol. 91:3, Springer, 1965, pp 265–284.

Department of Mathematics, African Institute for Mathematical science, Ghana
E-mail address: theophilus@aims.edu.gh/emperordagama@yahoo.com

[1] .