A LOWER BOUND FOR LENGTH OF ADDITION CHAINS

T. AGAMA

ABSTRACT. In this paper we show that the shortest length $\iota(n)$ of addition chains producing numbers of the form $2^n - 1$ satisfies the lower bound

$$\iota(2^n - 1) \geq n + \lfloor \frac{\log(n-1)}{\log 2} \rfloor$$

where $\lfloor \cdot \rfloor$ denotes the floor function.

1. Introduction

An addition chain producing $n \geq 3$, roughly speaking, is a sequence of numbers of the form $1, 2, s_3, s_4, \ldots, s_{k-1}, s_k = n$ where each term is the sum of two earlier terms in the sequence, obtained by adding each sum generated to an earlier term in the sequence. The number of terms in the sequence excluding n is the length of the chain. There are quite a number of addition chains producing a fixed number n. Among them the shortest is regarded as the shortest or optimal addition chain producing n. Nonetheless minimizing an addition chain can be an arduous endeavour, given that there are currently no efficient method for obtaining the shortest addition producing a given number. This makes the theory of addition chains an interesting subject to study. By letting $\iota(n)$ denotes the length of the shortest addition chain producing n, Arnold scholz conjectured the inequality

Conjecture 1.1 (Scholz). *The inequality holds*
$$\iota(2^n - 1) \leq n - 1 + \iota(n).$$

It has been shown computationally that the conjecture holds for all $n \leq 5784688$ and in fact it is an equality for all $n \leq 64$ [2]. Alfred Brauer proved the scholz conjecture for the star addition chain, an addition chain where each term obtained by summing uses the immediately subsequent number in the chain. By denoting the shortest length of the star addition chain by $\iota^*(n)$, it is shown that (See,[1])

Theorem 1.2. *The inequality holds*
$$\iota^*(2^n - 1) \leq n - 1 + \iota^*(n).$$

In this paper we study an addition chain of a fixed degree, a generalization of addition chains. We call an addition chain of degree d a sequence of numbers of the form $1, 2, s_3, s_4, \ldots, s_{k-1}, s_k = n$, where each term in the sequence is the sum of at most d previous terms in the sequence. In this paper, we study short addition

chains of degree $\lfloor \frac{n-1}{2} \rfloor$ producing numbers of the form $2^n - 1$ and prove an analogue of Scholz's conjecture on this chain. We obtain the inequality

Corollary 1.3. *Let $\iota(n)$ denotes the length of the shortest addition chain producing n. Then we have the lower bound*

$$\iota(2^n - 1) \geq n + \lfloor \frac{\log(n-1)}{\log 2} \rfloor$$

where $\lfloor \cdot \rfloor$ denotes the floor function.

2. Addition chains of fixed degree

In this section, we introduce the notion of addition chains of degree d and their corresponding sub-addition chains. We first recall the following notion of an addition chains.

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 $(j \geq 2)$ in the sequence is the **sum** of two earlier terms in the sequence, with the corresponding sequence of partition

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

with $a_{i+1} = a_i + r_i$ and $a_{i+1} = s_i$ for $2 \leq i \leq k$. We call the partition $a_i + r_i$ the ith **generator** of the addition chain of degree d for $2 \leq i \leq k$. We call a_i the **determiner** and r_i the **regulator** of the ith generator of the chain. We call the sequence (r_i) the regulators of an addition chain and (a_i) the determiners of the addition chain for $2 \leq i \leq k$.

Remark 2.2. We now introduce the notion of addition chains of degree d producing a fixed number n. This type of addition chain can be considered as a generalization of addition chains where we allow each term in the chain to be the sum of at most d earlier terms in the chain. The notion of an addition is the situation where we take $d = 1$. We make this notion formal and apply to some problems in the sequel.

Definition 2.3. Let $n \geq 3$, then by the addition chain of degree d and 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 at most d earlier terms, with the corresponding sequence of partition

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

with $a_{i+1} = a_i + r_i$ and $a_{i+1} = s_i$ for $2 \leq i \leq k$, where

$$r_i = \sum_{m \in [1,d]} s_m$$

for $i \leq d$. 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 **block** determiners of length at most $d+1$ and r_i the **block** regulator of length at most d of the i th generator of the chain. We call the sequence (r_i) the **block** regulators of the addition chain and (a_i) the **block** determiners of the chain for $2 \leq i \leq k$.

The notion above is a generalization of the notion of the regulators and the determiners of an addition to the setting of an addition chain of degree d. In this case, the regulator is viewed as a partition of at most d previous terms and each determiner the partition of at most $d+1$ previous terms in the sequence. In the situation where we allow $d = 1$, then the block regulators and the block determiners coincides with regulators and determiners of an addition chain.

Definition 2.4. Let the sequence $1, 2, \ldots, s_{k-1}, s_k = n$ be an addition chain producing n with the corresponding sequence of partition

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

Then we call the sub-sequence (s_{j_m}) for $1 \leq j \leq k$ and $1 \leq m \leq t \leq k$ a **sub-addition** chain of degree d of the addition chain of degree d producing n. We say it is a **complete** sub-addition chain of degree d of the addition chain of degree d producing n if it contains exactly the first t terms of the addition chain of degree d. Otherwise, we say it is an **incomplete** sub-addition chain of degree d.

2.1. **Addition chains of degree d of numbers of special forms.** In this section we study addition chains of a fixed degree of numbers of special forms. We examine ways of minimizing the length of the addition chain of degree $\lfloor \frac{n-1}{2} \rfloor$ for numbers of the form $2^n - 1$.

Lemma 2.5. *Let $\iota(n)$ and $\iota^{\lfloor \frac{n-1}{2} \rfloor}(n)$ denotes the length of the shortest addition chain and addition chain of degree $\lfloor \frac{n-1}{2} \rfloor$, respectively, producing n. Then the inequality*

$$\iota(2^n - 1) \geq \iota^{\lfloor \frac{n-1}{2} \rfloor}(2^n - 1)$$

holds.

Remark 2.6. We now obtain an analogous inequality for addition chains of degree $\lfloor \frac{n-1}{2} \rfloor$ producing $2^n - 1$ related to the scholz conjecture.

3. **The lower bound**

In this section, we prove an analogue of the scholz conjecture on addition chains of degree $\lfloor \frac{n-1}{2} \rfloor$.

Theorem 3.1. *Let $\iota(n)$ and $\iota^{\lfloor \frac{n-1}{2} \rfloor}(n)$ denotes the length of the shortest addition chain and addition chain of degree $\lfloor \frac{n-1}{2} \rfloor$, respectively, producing n. Then the identity*

$$\iota^{\lfloor \frac{n-1}{2} \rfloor}(2^n - 1) = n + \lfloor \frac{\log(n-1)}{\log 2} \rfloor$$

holds.

Proof. First, let us construct the shortest addition chain producing 2^n as $1, 2, 2^2, \ldots, 2^{n-1}, 2^n$ with corresponding sequence of partition

$$2 = 1 + 1, 2 + 2 = 2^2, 2^2 + 2^2 = 2^3 \ldots, 2^{n-1} = 2^{n-2} + 2^{n-2}, 2^n = 2^{n-1} + 2^{n-1}$$

with $a_i = 2^{i-2} = r_i$ for $2 \leq i \leq n+1$, where a_i and r_i denotes the determiner and the regulator of the ith generator of the chain. Let us consider only the complete sub-addition chain $1, 2, 2^2, \ldots, 2^{n-1}$. Next we extend this addition chain by adjoining the sequence

$$2^{n-1} + \cdots + 2^{t_1} + \cdots + 2^{\lfloor \frac{n-1}{2} \rfloor}, 2^{n-1} + \cdots + 2^{t_1} + \cdots + 2^{\lfloor \frac{n-1}{2} \rfloor} + \cdots + 2^{t_2} + \cdots + 2^{\lfloor \frac{n-1}{2^2} \rfloor},$$

$$(3.1)$$

$$\ldots, 2^{n-1} + 2^{n-2} + 2^{n-3} + \cdots + 2^1.$$

where $\lfloor \frac{n-1}{2} \rfloor + 1 \leq t_1 \leq n-2$, $\lfloor \frac{n-1}{2^2} \rfloor + 1 \leq t_2 \leq \lfloor \frac{n-1}{2} \rfloor - 1, \ldots, \lfloor \frac{n-1}{2^k} \rfloor + 1 \leq t_k \leq \lfloor \frac{n-1}{2^{k-1}} \rfloor - 1$. The terms adjoined to the addition chain constructed can be recast into the forms

$$2^{n-1} + \cdots + 2^{t_1} + \cdots + 2^{\lfloor \frac{n-1}{2} \rfloor} = 2^n - 2^{\lfloor \frac{n-1}{2} \rfloor}$$

and

$$2^{n-1} + \cdots + 2^{t_1} + \cdots + 2^{\lfloor \frac{n-1}{2} \rfloor} + \cdots + 2^{t_2} + \cdots + 2^{\lfloor \frac{n-1}{2^2} \rfloor} = 2^n - 2^{\lfloor \frac{n-1}{2^2} \rfloor}$$

so that by induction we can write

$$2^{n-1} + 2^{n-2} + 2^{n-3} + \cdots + 2^1 = 2^n - 2$$

and we obtain the addition chain of degree $\lfloor \frac{n-1}{2} \rfloor$

$$1, 2, 2^2, \ldots, 2^{n-1}, 2^n - 2^{\lfloor \frac{n-1}{2} \rfloor}, 2^n - 2^{\lfloor \frac{n-1}{2^2} \rfloor}, \ldots, 2^n - 2, 2^n - 1.$$

We note that the adjoined sequence contributes

$$\lfloor \frac{\log(n-1)}{\log 2} \rfloor$$

terms to the original complete addition chain. This completes the proof. □

Corollary 3.2. *Let $\iota(n)$ denotes the length of the shortest addition chain producing n. Then we have the lower bound*

$$\iota(2^n - 1) \geq n + \lfloor \frac{\log(n-1)}{\log 2} \rfloor$$

where $\lfloor \cdot \rfloor$ denotes the floor function.

Proof. The inequality follows by appealing to Lemma 2.5 in Theorem 3.1. □

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, 2011, pp 265–284.

DEPARTMENT OF MATHEMATICS, AFRICAN INSTITUTE FOR MATHEMATICAL SCIENCES, GHANA.
E-mail address: Theophilus@aims.edu.gh/emperordagama@yahoo.com