A PROOF OF THE SCHOLZ CONJECTURE ON ADDITION CHAINS

THEOPHILUS AGAMA

Abstract. Applying the pothole method on the factors of numbers of the form $2^n - 1$, we prove the inequality

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

where $\iota(n)$ denotes the length of the shortest addition chain producing n.

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 length of the chain is determined by the number of entries in the sequence excluding n. There are numerous addition chains that result in a fixed number n. The shortest or optimal addition chain produces n. However, given that there is currently no efficient method for getting the shortest addition yielding a given number, reducing an addition chain might be a difficult task. This makes addition chain theory a fascinating subject to study. Arnold Scholz conjectured the inequality by letting $\iota(n)$ denote the length of the shortest addition chain producing n.

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 1.1. *The inequality holds*

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

In this paper we combine the factor method and the "fill in the pothole" method to study short addition chains producing numbers of the form $2^n - 1$ and the Scholz

Date: December 1, 2022.

2010 *Mathematics Subject Classification.* Primary 11P83, 11B50 ; Secondary 11B75, 11B30.

Key words and phrases. sub-addition chain; determiners; regulators; length; generators; partition; complete.

conjecture. Given any number of the form $2^n - 1$, we obtain the decomposition

$$2^n - 1 = (2^{\frac{n-(1-(-1)^n)\frac{1}{2}}{2}} - 1)(2^{\frac{n-(1-(-1)^n\frac{1}{2})}{2}} + 1) + \frac{(1-(-1)^n)}{2}(2^{n-(1-(-1)^n)\frac{1}{2}})$$

which eventually yield the following decomposition $2^n - 1 = (2^{\frac{n}{2}} - 1)(2^{\frac{n}{2}} + 1)$ in the case $n \equiv 0 \pmod 2$ and

$$2^n - 1 = (2^{\frac{n-1}{2}} - 1)(2^{\frac{n-1}{2}} + 1) + 2^{n-1}$$

in the case $n \equiv 1 \pmod 2$. We iterate this decomposition up to a certain desired frequency and apply the factor method on all the factors obtained from this decomposition. We then apply the pothole method to obtain a bound for the shortest addition chains producing the only factor of form $2^v - 1$. The length of the shortest addition chains of numbers of the form $2^v + 1$ is easy to construct, by first constructing the shortest addition chain producing 2^v, adding the first term of the chain to the last term and adjoining to the chain. We combine the method of **filling the potholes** and the factor method to prove the Scholz conjecture on length of addition chain producing $2^n - 1$.

2. **Sub-addition chains**

In this section we introduce the notion of sub-addition chains.

Definition 2.1. Let $n \geq 3$, then by the 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, 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 $2 \leq i \leq k$. 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 **determiners** 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 $2 \leq i \leq k$.

Definition 2.2. 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 the addition chain producing n. We say it is **complete** sub-addition chain of the addition chain producing n if it contains exactly the first t terms of the addition chain. Otherwise we say it is an **incomplete** sub-addition chain.

2.1. **Summary sketch and idea of proof.**

In this section we describe the method of **filling the potholes** which is employed to obtain our upper bound. We lay them down chronologically as follows.

- We first construct a complete sub-addition chain producing 2^n-1. For technical reasons which will become clear later, we stop the chain prematurely at 2^{n-1}.
- We extend this addition chain by a length of logarithm order.
- This extension has missing terms to qualify as addition chain producing 2^n-1. We fill in the missing terms thereby obtaining what one might refer to as spoof addition chain producing 2^n-1.
- Creating this spoof addition chain comes at a cost. The remaining step will be to cover the cost and render an account to obtain the upper bound.

3. **Addition chains of numbers of special forms and Main result**

In this section, we prove an explicit upper bound for the length of the shortest addition chain producing numbers of the form 2^n-1. We begin with the following important but fundamental result.

Lemma 3.1. *Let $\iota(n)$ denotes the length of the shortest addition chain producing n. Then we have the inequality*

$$\lfloor \frac{\log n}{\log 2} \rfloor \leq \iota(n).$$

Proof. The proof of this Lemma can be found in [1]. □

Lemma 3.2. *Let $\iota(n)$ denotes the length of the shortest addition chain producing n. If $a,b \in \mathbb{N}$ then*

$$\iota(ab) \leq \iota(a)+\iota(b).$$

Proof. The proof of this Lemma can be found in [1]. □

Theorem 3.3. *The inequality*

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

holds for all $n \in \mathbb{N}$ with $n \geq 2$, where $\iota(\cdot)$ denotes the length of the shortest addition chain producing $\cdot$.

Proof. First, we consider the number 2^n-1 and obtain the decomposition

$$2^n-1=(2^{\frac{n-(1-(-1)^n)\frac{1}{2}}{2}}-1)(2^{\frac{n-(1-(-1)^n\frac{1}{2})}{2}}+1)+\frac{(1-(-1)^n)}{2}(2^{n-(1-(-1)^n)\frac{1}{2}}).$$

It is easy to see that we can recover the general factorization of 2^n-1 from this identity according to the parity of the exponent n. In particular, if $n \equiv 0 \pmod 2$, then we have

$$2^n-1=(2^{\frac{n}{2}}-1)(2^{\frac{n}{2}}+1)$$

and

$$2^n-1=(2^{\frac{n-1}{2}}-1)(2^{\frac{n-1}{2}}+1)+2^{n-1}$$

if $n \equiv 1 \pmod 2$. By combining both cases, we obtain the inequality

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

obtained by constructing an addition chain producing $2^{n-1}-1$, adding $2^{n-1}-1$ to $2^{n-1}-1$, adding 1 and adjoining the result in the case $n \equiv 1 \pmod 2$. Applying Lemma 3.2, we obtain further the inequality

$$\iota(2^n-1) \leq \iota(2^{\frac{n-(1-(-1)^n)\frac{1}{2}}{2}}-1)+\iota(2^{\frac{n-(1-(-1)^n)\frac{1}{2}}{2}}+1)+2 \tag{3.1}$$

Again let us set $\frac{n-(1-(-1)^n)\frac{1}{2}}{2}=k$ in (3.1), then we obtain the general decomposition

$$2^k-1=(2^{\frac{k-(1-(-1)^k)\frac{1}{2}}{2}}-1)(2^{\frac{k-(1-(-1)^k\frac{1}{2})}{2}}+1)+\frac{(1-(-1)^k)}{2}(2^{k-(1-(-1)^k)\frac{1}{2}}).$$

It is easy to see that we can recover the general factorization of 2^k-1 from this identity according to the parity of the exponent k. In particular, if $k \equiv 0 \pmod 2$, then we have

$$2^k-1=(2^{\frac{k}{2}}-1)(2^{\frac{k}{2}}+1)$$

and

$$2^k-1=(2^{\frac{k-1}{2}}-1)(2^{\frac{k-1}{2}}+1)+2^{k-1}$$

if $k \equiv 1 \pmod 2$. By combining both cases, we obtain the inequality

$$\iota(2^k-1) \leq \iota((2^{\frac{k-(1-(-1)^k)\frac{1}{2}}{2}}-1)(2^{\frac{k-(1-(-1)^k\frac{1}{2})}{2}}+1))+2$$

obtained by constructing an addition chain producing $2^{k-1}-1$, adding $2^{k-1}-1$ to $2^{k-1}-1$, adding 1 and adjoining the result in the case $k \equiv 1 \pmod 2$. Applying Lemma 3.2, we obtain further the inequality

$$\begin{aligned}\iota(2^k-1) &\leq \iota(2^{\frac{k-(1-(-1)^k)\frac{1}{2}}{2}}-1)+\iota(2^{\frac{k-(1-(-1)^k)\frac{1}{2}}{2}}+1)+2\\ &=\iota(2^{\frac{n}{4}-(1-(-1)^n)\frac{1}{4}-(1-(-1)^k)\frac{1}{4}}-1)+\iota(2^{\frac{n}{4}-(1-(-1)^n)\frac{1}{4}-(1-(-1)^k)\frac{1}{4}}+1)+2 \qquad (3.2)\end{aligned}$$

so that by inserting (3.2) into (3.1), we obtain the inequality

$$\begin{aligned}\iota(2^n-1) &\leq \iota(2^{\frac{n}{4}-(1-(-1)^n)\frac{1}{4}-(1-(-1)^k)\frac{1}{4}}-1)+\iota(2^{\frac{n}{4}-(1-(-1)^n)\frac{1}{4}-(1-(-1)^k)\frac{1}{4}}+1)+2\\ &+\iota(2^{\frac{n-(1-(-1)^n)\frac{1}{2}}{2}}+1)+2. \qquad (3.3)\end{aligned}$$

Next we iterate the factorization to obtain

$$\begin{aligned}\iota(2^n-1) \leq \iota(2^{\frac{n-(1-(-1)^n)\frac{1}{2}}{2}}+1)+2+\iota(2^{\frac{n}{4}-(1-(-1)^n)\frac{1}{4}-(1-(-1)^k)\frac{1}{4}}+1)+2\\ ++\cdots+\iota(2^{\frac{n}{2^s}-\xi(n,s)}-1)+\iota(2^{\frac{n}{2^s}-\xi(n,s)}+1)+2 \qquad (3.4)\end{aligned}$$

where $0 \leq \xi(n,s) \leq 1$. It follows from (3.4) the inequality

$$\begin{aligned}\iota(2^n-1) &\leq \sum_{v=1}^{s}\frac{n}{2^v}+2s-\theta(n,s)+\iota(2^{\frac{n}{2^s}-\xi(n,s)}-1)\\ &=n(1-\frac{1}{2^{s-1}})+2s-\theta(n,s)+\iota(2^{\frac{n}{2^s}-\xi(n,s)}-1) \qquad (3.5)\end{aligned}$$

for some $0 \leq \theta(n,s)$ and $s < \lfloor\frac{\log n}{\log 2}\rfloor$. It is important to note that one of the s term is obtained by noting that there are at most $\frac{1}{2}s$ terms with odd exponents under the iteration process and each term with odd exponent contributes 2, and the other comes from summing 1 with frequency s finding the total length of the short addition chains producing numbers of the form 2^v+1. Now we set $k=$

$\frac{n}{2^s} - \xi(n,s)$ and construct the addition chain producing 2^k as $1, 2, 2^2, \ldots, 2^{k-1}, 2^k$ with corresponding sequence of partition

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

with $a_i = 2^{i-2} = r_i$ for $2 \leq i \leq k+1$, where a_i and r_i denotes the determiner and the regulator of the i^{th} generator of the chain. Let us consider only the complete sub-addition chain

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

Next we extend this complete sub-addition chain by adjoining the sequence

$$2^{k-1}+2^{\lfloor\frac{k-1}{2}\rfloor}, 2^{k-1}+2^{\lfloor\frac{k-1}{2}\rfloor}+2^{\lfloor\frac{k-1}{2^2}\rfloor}\ldots, 2^{k-1}+2^{\lfloor\frac{k-1}{2}\rfloor}+2^{\lfloor\frac{k-1}{2^2}\rfloor}+\cdots+2^1.$$

We note that the adjoined sequence contributes at most

$$\lfloor\frac{\log k}{\log 2}\rfloor < \lfloor\frac{\log n - s\log 2}{\log 2}\rfloor = \lfloor\frac{\log n}{\log 2}\rfloor - s \leq \iota(n) - s$$

terms to the original complete sub-addition chain, where the upper bound follows by virtue of Lemma 3.1. Since the inequality holds

$$\begin{aligned} 2^{k-1}+2^{\lfloor\frac{k-1}{2}\rfloor}+2^{\lfloor\frac{k-1}{2^2}\rfloor}+\cdots+2^1 &< \sum_{i=1}^{k-1} 2^i \\ &= 2^k - 2 \end{aligned}$$

we insert terms into the sum

$$2^{k-1}+2^{\lfloor\frac{k-1}{2}\rfloor}+2^{\lfloor\frac{k-1}{2^2}\rfloor}+\cdots+2^1 \tag{3.6}$$

so that we have

$$\sum_{i=1}^{k-1} 2^i = 2^k - 2.$$

Let us now analyze the cost of filling in the missing terms of the underlying sum. We note that we have to insert $2^{k-2}+2^{k-3}+\cdots+2^{\lfloor\frac{k-1}{2}\rfloor+1}$ into (3.6) and this is comes at the cost of adjoining

$$k-2-\lfloor\frac{k-1}{2}\rfloor$$

terms to the term in (3.6). The last term of the adjoined sequence is given by

$$2^{k-1}+(2^{k-2}+2^{k-3}+\cdots+2^{\lfloor\frac{k-1}{2}\rfloor+1})+2^{\lfloor\frac{k-1}{2}\rfloor}+2^{\lfloor\frac{k-1}{2^2}\rfloor}+\cdots+2^1. \tag{3.7}$$

Again we have to insert $2^{\lfloor\frac{k-1}{2}\rfloor-1}+\cdots+2^{\lfloor\frac{k-1}{2^2}\rfloor+1}$ into (3.7) and this comes at the cost of adjoining

$$\lfloor\frac{k-1}{2}\rfloor - \lfloor\frac{k-1}{2^2}\rfloor - 1$$

terms to the term in (3.7). The last term of the adjoined sequence is given by

$$2^{k-1}+(2^{k-2}+2^{k-3}+\cdots+2^{\lfloor\frac{k-1}{2}\rfloor+1})+2^{\lfloor\frac{k-1}{2}\rfloor}+(2^{\lfloor\frac{k-1}{2}\rfloor-1}+\cdots+2^{\lfloor\frac{k-1}{2^2}\rfloor+1})+2^{\lfloor\frac{k-1}{2^2}\rfloor}+\cdots+2^1. \tag{3.8}$$

By iterating the process, it follows that we have to insert into the immediately previous term by inserting into (3.8) and this comes at the cost of adjoining

$$\lfloor \frac{k-1}{2^j} \rfloor - \lfloor \frac{k-1}{2^{j+1}} \rfloor - 1$$

terms to the term in (3.8) for $j \leq \lfloor \frac{\log n}{\log 2} \rfloor - s$ since we are filling in at most $\lfloor \frac{\log k}{\log 2} \rfloor$ blocks with $k = \frac{n}{2^s} - \xi(n,s)$. It follows that the contribution of these new terms is at most

$$k - 1 - \left\lfloor \frac{k-1}{2^{\lfloor \frac{\log k}{\log 2} \rfloor}} \right\rfloor - \lfloor \frac{\log k}{\log 2} \rfloor \tag{3.9}$$

obtained by adding the numbers in the chain

$$k - 1 - \lfloor \frac{k-1}{2} \rfloor - 1$$

$$\lfloor \frac{k-1}{2} \rfloor - \lfloor \frac{k-1}{2^2} \rfloor - 1$$

::::::::::::
....

::::::::::::
....

$$\lfloor \frac{k-1}{2^{\lfloor \frac{\log k}{\log 2} \rfloor}} \rfloor - \lfloor \frac{k-1}{2^{\lfloor \frac{\log k}{\log 2} \rfloor + 1}} \rfloor - 1.$$

By undertaking a quick book-keeping, it follows that the total number of terms in the constructed addition chain producing $2^k - 1$ with $k = \frac{n}{2^s} - \xi(n,s)$ is

$$\begin{aligned}
\delta(2^k - 1) &\leq k + k - 1 - \left\lfloor \frac{k-1}{2^{\lfloor \frac{\log k}{\log 2} \rfloor + 1}} \right\rfloor - \lfloor \frac{\log k}{\log 2} \rfloor + \iota(n) - s \\
&\leq \frac{n}{2^{s-1}} - 1 - \left\lfloor \frac{\frac{n}{2^s} - \xi(n,s) - 1}{2^{\lfloor \frac{\log n}{\log 2} \rfloor + 1 - s}} \right\rfloor - \lfloor \frac{\log n}{\log 2} \rfloor + s + \iota(n) - s \\
&= \frac{n}{2^{s-1}} - 1 - \left\lfloor \frac{\frac{n}{2^s} - \xi(n,s) - 1}{2^{\lfloor \frac{\log n}{\log 2} \rfloor + 1 - s}} \right\rfloor - \lfloor \frac{\log n}{\log 2} \rfloor + \iota(n). \qquad (3.10)
\end{aligned}$$

By plugging the inequality (3.10) into the inequalities in (3.5) and noting that $\iota(\cdot) \leq \delta(\cdot)$, we obtain the inequality

$$\begin{aligned}
\iota(2^n - 1) &\leq \sum_{v=1}^{s} \frac{n}{2^v} + 2s - \theta(n,s) + \iota(2^{\frac{n}{2^s} - \xi(n,s)} - 1) \\
&= n - 1 + 2s - \lfloor \frac{\log n}{\log 2} \rfloor - \theta(n,s) - \left\lfloor \frac{\frac{n}{2^s} - \xi(n,s) - 1}{2^{\lfloor \frac{\log n}{\log 2} \rfloor + 1 - s}} \right\rfloor + \iota(n).
\end{aligned}$$

By taking s to be the greatest integer such that $2^{2s} \leq n$, then $2s \leq \lfloor \frac{\log n}{\log 2} \rfloor$ with

$$\left\lfloor \frac{\frac{n}{2^s} - \xi(n,s) - 1}{2^{\lfloor \frac{\log n}{\log 2} \rfloor + 1 - s}} \right\rfloor = 0$$

and we obtained further the inequality

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

since $0 \leq \theta(n,s)$ and the claimed inequality follows as a consequence. □

[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 science, Ghana
E-mail address: theophilus@aims.edu.gh/emperordagama@yahoo.com

[1] .