A REFINED POTHOLE METHOD AND 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

$$\iota(2^n-1)\leq \frac{3}{2}n-\left\lfloor \frac{n-2}{2^{\lfloor \frac{\log n}{\log 2}-1\rfloor+1}}\right\rfloor-\lfloor \frac{\log n}{\log 2}-1\rfloor+\frac{1}{4}(1-(-1)^n)+\iota(n)$$

where $\lfloor \cdot \rfloor$ denotes the floor function and $\iota(n)$ 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*

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

Date: November 23, 2022.

2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.

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

In this paper we study short addition chains producing numbers of the form 2^n-1 and the Scholz conjecture. We adopt the method of **filling the potholes** to obtain an explicit improved upper bound for an addition chain producing 2^n-1. This method by itself never really helped to obtain an upper bound of this type. In order to improve on the previous bound via this method, we will consider the numbers of the form 2^n-1 and carry out a certain decomposition according to the parity of the exponents n. For each of these specific decomposition - informed by choice of exponents - we apply the pothole method on individual factors, so that by applying an inequality of Alfred Braurer one can get some control on the length of the addition chain producing the individual factors. The situation becomes a little less straight-forward in the odd case, where some partition is carried out at the compromise of a longer addition chain.

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 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 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*

$$\iota(2^n - 1) \leq \frac{3}{2}n - \left\lfloor \frac{n-2}{2^{\lfloor \frac{\log n}{\log 2} - 1 \rfloor + 1}} \right\rfloor - \lfloor \frac{\log n}{\log 2} - 1 \rfloor + \frac{1}{4}(1 - (-1)^n) + \iota(n)$$

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

Proof. First, we consider the number $2^n - 1$ and examine the length of the addition chain according to the parity of the exponents n. If $n \equiv 0 \mod 2$ then we obtain the factorization

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

By setting $\frac{n}{2} = k$, we 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

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

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

$$2^{k-1}+2^{\lfloor \frac{k-1}{2} \rfloor}+2^{\lfloor \frac{k-1}{2^2} \rfloor}+\cdots+2^1 \tag{3.1}$$

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 (3.1) and this is comes at the cost of adjoining

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

terms to the term in (3.1). The last term of the adjoined sequence is given by

$$2^{k-1}+(2^{k-2}+2^{k-3}+\cdots+2^{\lfloor \frac{k-1}{2} \rfloor+1})+2^{\lfloor \frac{k-1}{2} \rfloor}+2^{\lfloor \frac{k-1}{2^2} \rfloor}+\cdots+2^1. \tag{3.2}$$

Again we have to insert $2^{\lfloor \frac{k-1}{2} \rfloor-1}+\cdots+2^{\lfloor \frac{k-1}{2^2} \rfloor+1}$ into (3.2) 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 (3.2). The last term of the adjoined sequence is given by

$$\begin{aligned} &2^{k-1}+(2^{k-2}+2^{k-3}+\cdots+2^{\lfloor \frac{k-1}{2} \rfloor+1})+2^{\lfloor \frac{k-1}{2} \rfloor}+(2^{\lfloor \frac{k-1}{2} \rfloor-1}+\cdots+2^{\lfloor \frac{k-1}{2^2} \rfloor+1})+2^{\lfloor \frac{k-1}{2^2} \rfloor}+ \\ &\cdots+2^1. \end{aligned} \tag{3.3}$$

By iterating the process, it follows that we have to insert into the immediately previous term by inserting into (3.3) and this comes at the cost of adjoining

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

terms to the term in (3.3) for $1 \leq s \leq \lfloor \frac{\log n}{\log 2}-1 \rfloor$ since we filling in at most $\lfloor \frac{\log k}{\log 2} \rfloor$ blocks with $k=\frac{n}{2}$. It follows that the contribution of these new terms is at most

$$k-1-\left\lfloor \frac{k-1}{2^{\lfloor \frac{\log k}{\log 2} \rfloor}} \right\rfloor-\lfloor \frac{\log k}{\log 2} \rfloor \tag{3.4}$$

obtained by adding the numbers in the chain

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

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

$$\vdots$$

$$\vdots$$

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

Appealing to Lemma 3.2 the inequality

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

holds for even n, where $\delta(\cdot)$ is the length of the constructed addition chain. By undertaking a quick book-keeping, it follows that the total number of terms in the constructed addition chain producing 2^k-1 with $k=\frac{n}{2}$ is

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

Now we construct an addition chain producing 2^k+1. We 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. By adding 1 to the last term of the chain, we obtain the addition chain producing 2^k+1 of the form $1,2,2^2,\ldots,$ $2^{k-1},2^k,2^k+1$ of length $k+1=\frac{n}{2}+1$. By combining the contribution of the length of the addition chains constructed, we obtain in the case $n\equiv 0 \pmod 2$ the inequality

$$\iota(2^n-1)\leq \frac{3}{2}n-\left\lfloor \frac{n-2}{2^{\lfloor \frac{\log n}{\log 2}-1\rfloor+1}}\right\rfloor - \lfloor \frac{\log n}{\log 2}-1\rfloor+\iota(n).$$

We now examine the case $n\equiv 1 \pmod 2$. In this case, we write

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

so that we construct an addition chain producing $2^{n-1}-1$. Once this addition chain is obtained, then we add the term $2^{n-1}-1$ to itself and finally add 1 to obtain the addition chain producing 2^n-1. It will follow from this construction that the length $\delta(2^n-1)$ is the sum of the length of the addition chain $\delta(2^{n-1}-1)$ and 2. Since $n-1\equiv 0 \pmod 2$, we can adapt the argument of the even case to obtain the upper bound

$$\delta(2^{n-1}-1)\leq \frac{3}{2}(n-1)-\left\lfloor \frac{n-3}{2^{\lfloor \frac{\log n}{\log 2}-1\rfloor+1}}\right\rfloor - \lfloor \frac{\log n}{\log 2}-1\rfloor+\iota(n)$$

so that the length

$$\iota(2^n-1)\leq \delta(2^{n-1}-1)+2=\frac{3}{2}(n-1)-\left\lfloor \frac{n-3}{2^{\lfloor \frac{\log n}{\log 2}-1\rfloor+1}}\right\rfloor - \lfloor \frac{\log n}{\log 2}-1\rfloor+\iota(n)$$

so that the length

$$\iota(2^n-1)\leq \frac{3}{2}n-\left\lfloor \frac{n-3}{2^{\lfloor \frac{\log n}{\log 2}-1\rfloor+1}}\right\rfloor - \lfloor \frac{\log n}{\log 2}-1\rfloor+\iota(n)+\frac{1}{2}.$$

The claimed inequality follows by combining both the even and the odd case. $\square$

[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] .