THE SCHOLZ CONJECTURE VIA A MULTI-STEP OPTIMIZATION

THEOPHILUS AGAMA

Abstract. An addition chain of length h that leads to an integer $n \geq 2$ is a strictly increasing sequence of positive integers $s_0 = 1, s_1 = 2, \ldots, s_h = n$ such that $s_i = s_j + s_k$ with $i > j \geq k \geq 0$ for each $i \in \{1, \ldots, h\}$. We denote the minimal length of an addition chain that leads to an integer target $\cdot$ by $\ell(\cdot)$. Combining a generalized version of the Brauer method with a multi-step minimization approach, we verify the speculative inequality

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

for all $n \geq 2$.

Contents

1. Introduction

The addition chains are arithmetic-combinatorial structures (sequences) whose studies have been motivated by their fundamental role in accelerating repeated exponentiation, an activity often encountered in various areas of cryptography [6, 7, 8, 9]. Formally speaking, an addition chain of length h that leads to a positive integer $n \geq 2$, introduced by the German mathematician (see, e.g., [2]) Arnold Scholz in 1937, is a strictly increasing sequence of positive integers

$$s_0 = 1, s_1 = 2, \ldots, s_h = n$$

such that $s_i = s_j + s_k$ with $i > j \geq k \geq 0$ for each $i \in \{1, \ldots, h\}$. The smallest positive integer s for which there exists an addition chain leading to $n \geq 2$ such that $\ell(n) = s$ is

Date: August 16, 2026.
2010 *Mathematics Subject Classification.* Primary 11Y55; Secondary 11Y16; 11B83.
Key words and phrases. multi-step minimization, arbitrary.

the minimal length of the chain. The central problem in studies of addition chains is the speculative inequality

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

conjectured by Arnold Scholz in his foundational studies [2]. This is now widely known as the Scholz conjecture on addition chains.

Various approaches to addressing the Scholz conjecture have been discovered and proposed, ranging from structural to digital-arithmetic approaches [10, 11, 12, 5]. Among the pool of digital-arithmetic approaches is the binary method which relies on developing the binary expansion of a target integer and constructing an addition that leads to the target in this form. This method (see, e.g., [10, 11, 13]) is widely used to make partial progress on the Scholz conjecture. Regardless of the underlying utility, it has obvious limitations that make the Scholz-Brauer problem not amenable to direct attack. Consequently, structural approaches tend to be the most tractable way to study the conjecture. It involves assigning sufficient conditions (see, e.g., [1, 3, 5]) to an addition chain that ensures that the minimal-length chain admitted by a chosen target integer n satisfies the Scholz-type inequality

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

The German mathematician Alfred Brauer (see, e.g, [1]) and Walter Hansen after him (see, e.g., [3]) were the pioneers of these structural pathways towards addressing the Scholz conjecture.

The Brauer addition chain of length h that leads to a positive integer $n \geq 2$ is an addition chain

$$s_0 = 1, s_1 = 2, \ldots, s_h = n$$

such that $s_i = s_{i-1} + s_j$ for each $i \in \{1, \ldots, h\}$. We denote the minimal length of a Brauer addition chain that leads to $\cdot$ by $\ell^*(\cdot)$. In [1], it is shown that the inequality

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

holds for all integers that admit a minimal-length Brauer addition chain. The key idea is to specify a minimal length addition chain that leads to n in the form

$$s_0 = 1, s_1 = 2, \ldots, s_{\ell^*(n)} = n$$

and lift each term in the chain via the rule $m_i := 2^{s_i} - 1$ in the following way

$$2^{s_0} - 1, 2^{s_1} - 1, \ldots, 2^{s_{\ell^*(n)}} - 1 = 2^n - 1.$$

The final and most crucial idea in the Brauer proof is to perform a certain repeated canonical doubling on each of the lifted terms $2^{s_i} - 1$ for each $0 \leq i \leq h - 1$. This process eventually produces a valid addition chain that leads to the *Mersenne* number $2^n - 1$. A careful bookkeeping of the contribution from the lifted terms and newly introduced terms that arise from the canonical doubling gives the Scholz-type inequality for this family of addition chains. [1]

In this paper, we use a similar "lifting" approach as a fundamental and guiding principle in our studies, but in a slightly different and adapted way. Rather than specifying a minimal-length chain that leads to a chosen target, we specify an arbitrary-length chain C_n that leads to a fixed target integer $n \geq 2$ and fix the terms that calculate each term in the

[1] For details, see the foundational paper of Alfred Brauer [1]

chain, considering the possibility of multiple pairs of terms that can generate the same term in the chain. For each admissible arbitrary length $\delta(n)$, we build a corresponding family of chains $F_{\delta(n),n}$ that lead to the target integer and fix an addition chain in each corresponding family. We then apply the Brauer construction to each fixed addition chain in each family with a fixed decomposition as a sum of two previous terms in the chain to construct a valid chain of the corresponding lifted chain that leads to the required *Mersenne* number as the target. By careful bookkeeping, we deduce

$$\ell(2^n - 1) \leq \min_{\ell(n)\leq\delta(n)\leq n-1} \left(\min_{F_{\delta(n),n}} \min_{H(C_n)} G(\delta(n), F_{\delta(n),n}, H(C_n)) + \delta(n) \right)$$

where $H(C_n)$ is a collection of vectors that arise from the "internal" structure of each addition chain C_n in the family $F_{\delta(n),n}$ and G is a function that depends on the statistics $\delta(n)$, $F_{\delta(n),n}$ and $H(C_n)$. This reduces the Scholz-Brauer problem to a purely optimization problem involving a multi-step minimization.

To approach this multi-step minimization problem, we rely on and borrow some ideas from the paper of Neill Clift including our own developed ideas that allow us to manage and decouple the double inner minimization. In his foundational computational-focused contribution (see, e.g., [4]), the addition chain and the Scholz-Brauer problem were studied using the graph theoretic-framework. There, the concepts of *graph reduction* and graph *expansion* were rigorously analyzed and studied. However, in this paper, the concept of *reduced* and *irreducible* addition chains has been introduced to eliminate redundant terms in an addition chain that leads to a target integer. It is worth remarking that the concept of *reduction* in our investigation and that in [4] are slightly different in their usage and scope and therefore should not be read as parallel ideas.

Informally, a *reducible* addition chain $C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$ is the one in which the chain can be shortened to a valid chain by removing a term from the chain. Otherwise, the addition chain is considered irreducible. For each term in the chain C_n with $s_i = s_j + s_k$ with $i > j \geq k$ for each $i \in \{1, \ldots, h\}$, we define the partial variation of the chain by

$$\mathbb{PV}(C_n) := \min_{H(C_n)} \left(\sum_{k\geq 0} s_k \right)$$

where $H(C_n)$ is the collection of all vectors of the indices of the lower weight summands that calculate each term of the chain C_n. [2]. It has been shown that

$$\mathbb{PV}(C_n) \leq n - 1 + P(C_n, h, m(h))$$

where $m(h)$ is a certain coefficient (multiplicity) in a linear combination of chain terms that depends on the length of the chain. For a minimal length chain, it is realized that $P(C_n, h, m(h)) \leq 0$. Our final step in establishing the Scholz-Brauer inequality reduces to showing that the double inner minimum function is exactly a minimization of the partial variation in the family of all admissible lengths of a chain leading to a fixed target $n \geq 2$.

1.1. **Organization of the paper.** The paper is organized as follows: Section 2 lays the background and framework for our studies, introducing the partial variation function, the internal structure of an addition chain as choices of σ and τ tracks of the chain. Section

[2]The collection of all vectors of indices of lower weight summands that calculate each chain term referred to will be specified in subsequent sections

3 introduces and develops the concept of reducibility and irreducibility of an addition chain. Here, we prove important observations of this concept by showing that every chain leading to a target integer has an irreducible chain and that chiefly a minimal-length chain is naturally an irreducible chain. Section 4 proves an inequality that relates the partial variation of a chain to the target integer and certain terms in the chain with a certain coefficient as their multiplicity. Here, we show that the partial variation of a minimal-length chain is at most a unit left shift of the target integer of the chain. The final section (section 5) assembles the ideas developed in the previous section in conjunction with the Brauer lifting approach to address the Scholz-Brauer problem via a multi-step minimization.

1.2. **Notation.**

(1) The function $\ell(\cdot)$ and $\delta(\cdot)$ will denote the length of a shortest and arbitrary addition chain that leads to a target integer $\cdot$.

(2) The function $\min_{x}(\cdot)$ minimizes $\cdot$ over all x.

(3) For any two sets A and B, the notation $A \setminus B$ is the standard set exclusion, which means the set of all elements in A that are not in B.

(4) The notation $\subseteq, \subset$ and $\cup$ denotes the usual subset sets and the union of sets.

2. Preliminary, background and motivation

Let

$$s_0 = 1 < s_1 = 2 < \cdots < s_h = n$$

be a fixed addition chain of length h leading to n together with the fixed decomposition $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $1 \leq i \leq h$ such that $s_{\sigma(0)} := s_0 = 1$ and $s_{\tau(0)} := 0$. We call the sequence $\{s_{\sigma(i)}\}_{i=1}^{h}$ a σ track and the sequence $\{s_{\tau(i)}\}_{i=1}^{h}$ a τ track of the addition chain. We say that a σ track is nondecreasing when

$$s_{\sigma(i)} \leq s_{\sigma(i+1)}$$

for each $1 \leq i \leq h-1$. Similarly, we say that a τ track is nondecreasing when

$$s_{\tau(i)} \leq s_{\tau(i+1)}$$

for each $1 \leq i \leq h-1$.

Example 2.1. Consider the addition chain $C_{16} : s_0 = 1, s_1 = 2, s_2 = 4, s_3 = 8, s_4 = 9, s_5 = 16$ with sums

$$\begin{aligned}
s_1 &= 2 = 1 + 1 = s_{\sigma(1)} + s_{\tau(1)} \\
s_2 &= 4 = 2 + 2 = s_{\sigma(2)} + s_{\tau(2)} \\
s_3 &= 8 = 4 + 4 = s_{\sigma(3)} + s_{\tau(3)} \\
s_4 &= 9 = 8 + 1 = s_{\sigma(4)} + s_{\tau(4)} \\
s_5 &= 16 = 8 + 8 = s_{\sigma(5)} + s_{\tau(5)}.
\end{aligned}$$

Here, the σ track $1 = s_{\sigma(1)} < s_{\sigma(2)} = 2 < s_{\sigma(3)} = 4 < s_{\sigma(4)} = 8 = s_{\sigma(5)}$ is not decreasing whereas the τ track is neither decreasing nor increasing.

Definition 2.2. Let $n \geq 2$ and $s_0 = 1, s_1 = 2, \ldots, s_h = n$ be a fixed addition chain leading to n. We say that $s_i < s_j$ for $1 \leq i, j, \leq h$ are consecutive terms in the addition chain if there are no terms s_k in the addition chain such that $s_i < s_k < s_j$. In particular, if $s_i < s_j$ are consecutive terms in the addition chain, then $i = j - 1$.

Definition 2.3 (The partial variation of an addition chain)**.** Let $n \geq 2$ be a fixed positive integer, and let

$$C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$$

be a fixed addition chain leading to n with decomposition $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $1 \leq i \leq h$, where $\sigma, \tau : \{1, \ldots, i\} \longrightarrow \{0, \ldots, i-1\}$. We define the *partial variation* of the chain as

$$\mathbb{PV}(C_n) = \min_{H(C_n)} \left(\sum_{i=1}^{h} s_{\tau(i)} \right)$$

where

$$H(C_n) = \left\{ \begin{pmatrix} \tau(1) \\ \tau(2) \\ \vdots \\ \tau(h) \end{pmatrix} \right\}$$

is the collection of all vectors of τ values with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ in the fixed addition chain C_n.

Here, we provide an example to illustrate the partial variation functional.

Example 2.4. We consider a minimal-length addition leading to 11

$$C_{11} : s_0 = 1, s_1 = 2, s_2 = 3, s_3 = 5, s_4 = 6, s_5 = 11$$

and observe the following possible sums that calculate each term in the chain

$$\begin{aligned} s_1 &= 2 = 1 + 1 = s_{\sigma(1)} + s_{\tau(1)} \\ s_2 &= 3 = 2 + 1 = s_{\sigma(2)} + s_{\tau(2)} \\ s_3 &= 5 = 3 + 2 = s_{\sigma(3)} + s_{\tau(3)} \\ s_4 &= 6 = 3 + 3 = s_{\sigma(4)} + s_{\tau(4)} \\ s_5 &= 11 = 6 + 5 = s_{\sigma(5)} + s_{\tau(5)} \end{aligned}$$

with the sum

$$\sum_{i=1}^{5} s_{\tau(i)} = 12$$

or

$$\begin{aligned} s_1 &= 2 = 1 + 1 = s_{\sigma(1)} + s_{\tau(1)} \\ s_2 &= 3 = 2 + 1 = s_{\sigma(2)} + s_{\tau(2)} \\ s_3 &= 5 = 3 + 2 = s_{\sigma(3)} + s_{\tau(3)} \\ s_4 &= 6 = 5 + 1 = s_{\sigma(4)} + s_{\tau(4)} \\ s_5 &= 11 = 6 + 5 = s_{\sigma(5)} + s_{\tau(5)} \end{aligned}$$

with the sum

$$\sum_{i=1}^{5} s_{\tau(i)} = 10.$$

The partial variation of the addition chain C_{11} is the minimum of the sums

$$\mathbb{PV}(C_{11}) = \min_{H(C_{11})} \left(\sum_{i=1}^{5} s_{\tau(i)} \right) = 10.$$

Theorem 2.5 (The partial variation method)**.** *Let $n \geq 2$ be a fixed positive integer, and let*

$$C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$$

be a fixed optimal addition chain leading to n with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $1 \leq i \leq h$. We have

$$\ell(2^n - 1) \leq \mathbb{PV}(C_n) + \ell(n).$$

If the partial variation

$$\mathbb{PV}(C_n) := \min_{H(C_n)} \left(\sum_{i=1}^{h} s_{\tau(i)} \right) \leq n - 1$$

then $\ell(2^n - 1) \leq n - 1 + \ell(n)$, where $\ell(\cdot)$ denotes the length of the shortest addition chain that leads to $\cdot$.

Proof. Let $s_0 = 1, s_1 = 2, \ldots, s_h = n$ be a fixed optimal addition chain leading to $n \geq 2$, and denote the length of the chain by $\ell(n)$. For now, we fix the decomposition $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $1 \leq i \leq h$. We now define $m_i = 2^{s_i} - 1$ for $i = 0, 1, \ldots, h$ and enumerate the sequence

$$2^{s_0} - 1 := 2^1 - 1, 2^{s_1} - 1 := 2^2 - 1, \ldots, 2^{s_h} - 1 = 2^n - 1.$$

We now build an addition chain leading to $2^n - 1$ using the above sequence as a building block. To do this, we perform a $(s_{i+1} - s_{\sigma(i+1)})$ repeated doubling of the term $2^{s_{\sigma(i+1)}} - 1$ for each $i \in \{0, \ldots, h-1\}$ and include the result of each doubling in the sequence. We claim that this construction yields an addition chain that leads to $2^n - 1$. To see this, we observe

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

for each $0 \leq i \leq h - 1$. The total length of the constructed addition chain is therefore

$$\sum_{i=0}^{h-1} s_{\tau(i+1)} + \ell(n).$$

Since the construction holds for any fixed decomposition of terms in the chain C_n, we deduce

$$\ell(2^n - 1) \leq \min_{H(C_n)} \left(\sum_{i=0}^{h-1} s_{\tau(i+1)} \right) + \ell(n) \leq \mathbb{PV}(C_n) + \ell(n).$$

The special case can be deduced from the inequality. □

Definition 2.6 (The τ and σ trace of an addition chain)**.** Let $n \geq 2$ be a fixed positive integer, and let $C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$ be any fixed addition chain that leads to n with a decomposition $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $1 \leq i \leq h$, where $\sigma, \tau : \{1, \ldots, i\} \longrightarrow \{0, \ldots, i-1\}$. We define the τ *trace* of the chain as

$$\mathbb{T}_{\tau}(C_n) := \max_{H(C_n)} \left(\sum_{i=1}^{h} s_{\tau(i)} \right).$$

Similarly, we define the σ trace of the chain as

$$\mathbb{T}_{\sigma}(C_n) := \max_{H(C_n)} \left(\sum_{i=1}^{h} s_{\sigma(i)} \right).$$

Here, the maximum is taken over the collection of all vectors

$$H(C_n) := \left\{ \begin{pmatrix} \tau(1) \\ \tau(2) \\ \vdots \\ \tau(h) \end{pmatrix} \right\}$$

and

$$L(C_n) := \left\{ \begin{pmatrix} \sigma(1) \\ \sigma(2) \\ \vdots \\ \sigma(h) \end{pmatrix} \right\}$$

of τ and σ values so that $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $1 \leq i \leq h$ for the fixed addition chain C_n.

3. Reduced and irreducible addition chains

In this section, we introduce and develop the concept of *reducible* and *irreducible addition chains*

Definition 3.1 (Reduced addition chains)**.** Let

$$s_0 = 1, s_1 = 2, \ldots, s_h = n$$

be a fixed addition chain of length h that leads to n together with the decomposition $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $i \in \{1, \ldots, h\}$. We say that the addition chain is *partially reducible* if there exists some choice of σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ such that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^{h} \cup \{s_{\tau(k)}\}_{k=1}^{h} \right) \right) \subset \{s_k\}_{k=0}^{h}$$

and

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^{h} \cup \{s_{\tau(k)}\}_{k=1}^{h} \right) \right)$$

is also an addition chain that leads to n when arranged in a strictly increasing order of magnitude. We say that the addition chain is *irreducible* when there is no choice of σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ so that the addition chain is partially reducible. Here, we call

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^{h} \cup \{s_{\tau(k)}\}_{k=1}^{h} \right) \right)$$

a *reduced* addition chain that leads to n. We say that the addition chain is *fully reducible* if the above condition holds for each choice of σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$. We call

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right)$$

a *reduced* addition chain that leads to n for each choice of the σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$.

Example 3.2. Consider the addition chain $s_0 = 1, s_1 = 2, s_2 = 3, s_3 = 5, s_4 = 6, s_5 = 10, s_6 = 12$ with sums

$$\begin{aligned}
s_1 &= 2 = 1 + 1 = s_{\sigma(1)} + s_{\tau(1)} \\
s_2 &= 3 = 2 + 1 = s_{\sigma(2)} + s_{\tau(2)} \\
s_3 &= 5 = 3 + 2 = s_{\sigma(3)} + s_{\tau(3)} \\
s_4 &= 6 = 3 + 3 = s_{\sigma(4)} + s_{\tau(4)} \\
s_5 &= 10 = 5 + 5 = s_{\sigma(5)} + s_{\tau(5)} \\
s_6 &= 12 = 10 + 2 = s_{\sigma(6)} + s_{\tau(6)}
\end{aligned}$$

The σ track is $\{1, 2, 3, 5, 10\}$ and the τ track $\{1, 2, 3, 5\}$. Therefore

$$\{s_k\}_0^6 \setminus \left(\{s_k\}_{k=0}^{5} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^6 \cup \{s_{\tau(k)}\}_{k=1}^6\right)\right) = \{1, 2, 3, 5, 10, 12\}.$$

Arranging in a strictly increasing order of magnitude, we find that

$$s_0 = 1, s_1 = 2, s_2 = 3, s_3 = 5, s_4 = 10, s_5 = 12$$

is a *reduced* addition chain.

Example 3.3. Consider the addition chain $s_0 = 1, s_1 = 2, s_2 = 3, s_3 = 5, s_4 = 6, s_5 = 10, s_6 = 12$ with sums

$$\begin{aligned}
s_1 &= 2 = 1 + 1 = s_{\sigma(1)} + s_{\tau(1)} \\
s_2 &= 3 = 2 + 1 = s_{\sigma(2)} + s_{\tau(2)} \\
s_3 &= 5 = 3 + 2 = s_{\sigma(3)} + s_{\tau(3)} \\
s_4 &= 6 = 3 + 3 = s_{\sigma(4)} + s_{\tau(4)} \\
s_5 &= 10 = 5 + 5 = s_{\sigma(5)} + s_{\tau(5)} \\
s_6 &= 12 = 6 + 6 = s_{\sigma(6)} + s_{\tau(6)}.
\end{aligned}$$

Here, the σ track is $\{1, 2, 3, 5, 6\}$ and the τ track is $\{1, 2, 3, 5, 6\}$. Therefore

$$\{s_k\}_0^6 \setminus \left(\{s_k\}_{k=0}^{5} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^6 \cup \{s_{\tau(k)}\}_{k=1}^6\right)\right) = \{1, 2, 3, 5, 6, 12\}.$$

Arranging in a strictly increasing order of magnitude, we find that

$$s_0 = 1, s_1 = 2, s_2 = 3, s_3 = 5, s_4 = 6, s_5 = 12$$

is a *reduced* addition chain.

Definition 3.4 (Reduced addition chain of a given type)**.** Let G be a property, and let

$$s_0 = 1, s_1 = 2, \ldots, s_h = n$$

be a fixed addition chain of type G of length h that leads to n together with the decomposition $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $i \in \{1, \ldots, h\}$. We say that the addition chain of type G is *partially reducible* if there exists some choice of σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ such that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right) \subset \{s_k\}_{k=0}^h$$

and

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right)$$

is also an addition chain of type G that leads to n when arranged in a strictly increasing order of magnitude. We say that the addition chain of type G is *irreducible* when there is no choice of σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ so that the addition chain of type G is partially reducible. Here, we call

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right)$$

a *reduced* addition chain of type G that leads to n. We say that the addition chain of type G is *fully reducible* if the above condition holds for each choice of σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$. We call

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right)$$

a *reduced* addition chain of type G that leads to n for each choice of the σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$.

Proposition 3.5. *Let G be a property, and let $n \geq 2$ admit an addition chain of type G. There exists an irreducible addition chain of type G leading to n.*

Proof. We suppose that every addition chain of type G is reducible and let

$$C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$$

be a fixed addition chain of type G in the family of all addition chains of type G that lead to n. This implies that the addition chain C_n is partially reducible. Hence, there exists some choice of σ track $\{s_{\sigma(i)}\}_{i=1}^h$ and τ track $\{s_{\tau(i)}\}_{i=1}^h$ with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ with $i > \sigma(i) \geq \tau(i) \geq 0$ such that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right) \subset \{s_k\}_{k=0}^h$$

so that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right)$$

is an addition chain of type G that leads to n when the terms are arranged in a strictly increasing order of magnitude. We denote this reduced addition chain by C_n' with length h'. We deduce $h' < h$. Since every addition chain of type G is reducible, we can iterate this argument to obtain the infinite descending sequence of integer length of further reduced addition chains of type G

$$h > h' > \cdots$$

towards zero. This is impossible. □

For a chosen integer target and an addition chain that leads to the chosen target, one can construct an *irreducible* addition chain as exemplified in the examples in the preceding examples. However, every minimal-length addition chain is naturally irreducible.

Proposition 3.6 (The minimality-irreducibility criterion)**.** *Let $C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$ be a fixed minimal-length addition chain that leads to n. The addition chain C_n is irreducible.*

Proof. Let C_n be a fixed minimal-length addition chain that leads to n. We suppose that the addition chain C_n is *reducible*. This implies that C_n is necessarily *partially reducible*. Hence, there exists some choice of σ and τ tracks with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ such that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right) \subset \{s_k\}_{k=0}^h$$

so that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^h \cup \{s_{\tau(k)}\}_{k=1}^h\right)\right)$$

is an addition chain that leads to n when the terms are arranged in strictly increasing order of magnitude. This is a reduced addition chain of length strictly less than the minimal length of the chain. This is impossible; hence, the minimal-length addition chain is *irreducible*. □

Although irreducible addition chains can potentially be realized from a fixed addition chain of type G in the family of addition chains of type G, there are chains of type G that are already irreducible. The classical family of chains that are *Brauer* chains is a particular example. Here, we show that each fixed *Brauer* addition chain is *irreducible*.

Proposition 3.7. *Let C_n be a fixed Brauer chain that leads to $n \geq 2$. The Brauer addition chain C_n is irreducible.*

Proof. Let $C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$ be a fixed *Brauer* addition chain that leads to $n \geq 2$ with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for $i > \sigma(i) \geq \tau(i) \geq 0$ for each $i \in \{1, \ldots, h\}$. Because the chain C_n is *Brauer*, we deduce that $\sigma(i) = i - 1$ for each $i \in \{1, \ldots, h\}$. Since the addition chain C_n has been fixed, the σ track $\{s_{\sigma(i)}\}_{i=1}^h := \{s_i\}_{i=0}^{h-1}$ is determined. Hence, the τ track $\{s_{\tau(i)}\}_{i=1}^h$ is also determined since $s_i - s_{i-1} = s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$. This implies

$$\{s_i\}_{i=0}^h \setminus \left(\{s_i\}_{i=0}^{h-1} \setminus \left(\{s_{\sigma(i)}\}_{i=1}^h \cup \{s_{\tau(i)}\}_{i=1}^h\right)\right) = \{s_i\}_{i=0}^h.$$

If we assume that the addition chain C_n is *reducible*, then

$$\{s_i\}_{i=0}^h \setminus \left(\{s_i\}_{i=0}^{h-1} \setminus \left(\{s_{\sigma(i)}\}_{i=1}^h \cup \{s_{\tau(i)}\}_{i=1}^h\right)\right) = \{s_i\}_{i=0}^h \subset \{s_i\}_{i=0}^h$$

which is impossible. □

Reduced addition chains of type G have a shorter length than their corresponding addition chain. However, they inherit important functional statistics from an addition chain of type G.

Proposition 3.8 (The reducibility trace inequality)**.** *Let $C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$ be an addition chain that leads to $n \geq 2$. Furthermore, let C_n' be a reduced addition chain of the addition chain C_n. The following properties hold:*

(1) $\mathbb{T}_\tau(C_n') \leq \mathbb{T}_\tau(C_n)$
(2) $\mathbb{T}_\sigma(C_n') \leq \mathbb{T}_\sigma(C_n)$.

Proof. Suppose that C_n' is a reduced addition chain of type G of the addition chain

$$C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$$

of type G. This implies that there exists some choice of σ track $\{s_{\sigma(i)}\}_{i=1}^{h}$ and τ track $\{s_{\tau(i)}\}_{i=1}^{h}$ with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$ such that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^{h} \cup \{s_{\tau(k)}\}_{k=1}^{h}\right)\right) \subset \{s_k\}_{k=0}^{h}$$

so that

$$\{s_k\}_0^h \setminus \left(\{s_k\}_{k=0}^{h-1} \setminus \left(\{s_{\sigma(k)}\}_{k=1}^{h} \cup \{s_{\tau(k)}\}_{k=1}^{h}\right)\right)$$

is the addition chain C_n' of type G that leads to n when the terms are arranged in a strictly increasing order of magnitude. The terms of the σ and τ tracks of the reduced addition chain C_n' of type G are also the terms of some choice of the σ and τ tracks of the addition chain C_n. However, it may be possible that there is a term in some choice of a σ and τ track of the addition chain C_n which is not a term of the σ and τ tracks of the reduced chain C_n'. The claimed inequalities follow from these assertions. □

3.1. **Reducibility and gap laws.** Let $C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$ be an addition chain that leads to $n \geq 2$. For any pair (s_j, s_k), we define the *gap* as the absolute difference

$$\Delta_{j,k} := |s_j - s_k|$$

In this section, we study the interplay between *irreducibility* and the gap between terms in an addition chain. In particular, we show that each term in an irreducible addition chain can be written as the difference of two terms in the chain.

Proposition 3.9 (Irreducibility-gap criterion)**.** *Let $C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$ be an irreducible addition chain that leads to $n \geq 2$. For each $i \in \{1, \ldots, h-1\}$, there exists a pair (s_j, s_k) of terms in the chain C_n such that*

$$\Delta_{j,k} := |s_j - s_k| = s_i.$$

Proof. We suppose that the addition chain

$$C_n : s_0 = 1, s_1 = 2, \ldots, s_h = n$$

is irreducible. This implies that for each choice of σ track $\{s_{\sigma(i)}\}_{i=1}^{h}$ and τ track $\{s_{\tau(i)}\}_{i=1}^{h}$ with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ for each $i \in \{1, \ldots, h\}$, we must have

$$\{s_i\}_{i=0}^{h-1} = \{s_{\sigma(i)}\}_{i=1}^{h} \cup \{s_{\tau(i)}\}_{i=1}^{h}.$$

Therefore, for each $s_k \in \{s_i\}_{i=0}^{h-1}$, we must have $s_k \in \{s_{\sigma(i)}\}_{i=1}^{h}$ or $s_k \in \{s_{\tau(i)}\}_{i=1}^{h}$. Without loss of generality, we let $s_k \in \{s_{\sigma(i)}\}_{i=1}^{h}$. Hence, there exists a pair (s_l, s_j) with $s_l \in \{s_i\}_{i=0}^{h}$ and $s_j \in \{s_{\tau(i)}\}_{i=1}^{h} \cup \{s_{\sigma(i)}\}_{i=1}^{h}$ so that

$$s_l = s_k + s_j \implies s_k = s_l - s_j := \Delta_{l,j}.$$

□

4. The partial variation inequality vs irreducibility

In this section, we develop an inequality that relates the *partial variation* of an addition chain to its target and "internal" structure.

Proposition 4.1 (The partial variation inequality)**.** *Let $C_n : s_0 = 1 < s_1 < \cdots < s_h = n$ be any fixed addition chain leading to n with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(\sigma(i) \geq \tau(i), 1 \leq i \leq h)$. Define the multiplicity*

$$m_t := \#\{i \in \{1, \ldots, h\} \ : \ \sigma(i) = t, 0 \leq t \leq h-1\}$$

which may be zero for some t. We have

$$\mathbb{PV}(C_n) \leq n - m_0 + \sum_{t=1}^{h-1}(1-m_t)s_t = n - 1 + \sum_{t=1}^{h-1}(1-m_t)s_t.$$

Proof. We set

$$m_t := \#\{i \in \{1, \ldots, h\} \ : \ \sigma(i) = t, 0 \leq t \leq h-1\}.$$

This is the number of times the index $\sigma(i)$ appears as indices for each term s_t as a dominant summand used to calculate a term in the chain, where $m_t \geq 0$. We write

$$\begin{aligned}
\mathbb{PV}(C_n) :&= \min_{H(C_n)}\left(\sum_{i=1}^{h} s_{\tau(i)}\right) \\
&\leq \sum_{i=1}^{h} s_{\tau(i)} \\
&= \sum_{i=1}^{h} s_i - \sum_{i=1}^{h} s_{\sigma(i)} \\
&= \sum_{t=1}^{h} s_t - \sum_{t=0}^{h-1} m_t s_t, \quad (\sigma(i) \in \{0, \ldots, i-1\}) \\
&= s_h - m_0 + \sum_{t=1}^{h-1}(1-m_t)s_t \\
&= n - m_0 + \sum_{t=1}^{h-1}(1-m_t)s_t.
\end{aligned}$$

□

Lemma 4.2 (The partial variation-irreducibility criterion)**.** *Let $C_n : s_0 = 1 < s_1 < \cdots < s_h = n$ be any fixed addition chain leading to n with $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(\sigma(i) \geq \tau(i), 1 \leq i \leq h)$. Define the multiplicity*

$$m_t := \#\{i \in \{1, \ldots, h\} \ : \ \sigma(i) = t, 0 \leq t \leq h-1\}$$

which may be zero for some t. If the addition chain C_n is irreducible, then

$$\sum_{t=1}^{h-1}(1-m_t)s_t \leq 0.$$

Proof. Suppose that the addition chain $C_n : s_0 = 1 < s_1 = 2 < \cdots < s_h = n$ is irreducible. This means that each term in the chain must be used at least once to calculate a subsequent term in the chain, which further implies $m_t \geq 1$. The inequality is deduced from this simple fact. □

5. The main result: proof of the Scholz conjecture

The current section approaches the Scholz-Brauer problem, namely the speculative inequality

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

using a multi-step optimization combined with a slight and a carefully adapted version of the partial variation method.

Theorem 5.1 (A multi-step minimization approach)**.** *For all $n \geq 2$, we have*

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

Proof. We let $n \geq 2$ be a fixed integer and let $\delta(\cdot)$ denote an arbitrary admissible length of an addition chain that leads to $\cdot$. Here, we observe that $\ell(n) \leq \delta(n) \leq n - 1$. The lower bound is attained for a minimal-length addition chain, and the upper bound is attained for the sequence of consecutive integers that lead to n

$$s_0 = 1, s_1 = 2, \ldots, s_{n-1} = n$$

which is also an addition chain with the greatest length $n - 1$. We let $F_{\delta(n),n}$ denote the family of all addition chains leading to n with an arbitrary admissible length $\delta(n)$. We fix an addition chain $C_n : s_0 = 1, s_1 = 2, \ldots, s_{\delta(n)} = n$ in each family $F_{\delta(n),n}$ for each choice of $\delta(n)$ and fix the decomposition $s_i = s_{\sigma(i)} + s_{\tau(i)}$ $(i > \sigma(i) \geq \tau(i) \geq 0)$ for each $1 \leq i \leq \delta(n)$. We now define $m_i = 2^{s_i} - 1$ for $i = 0, 1, \ldots, \delta(n)$ and enumerate the sequence

$$2^{s_0} - 1 := 2^1 - 1, 2^{s_1} - 1 := 2^2 - 1, \ldots, 2^{s_{\delta(n)}} - 1 = 2^n - 1.$$

We now build an addition chain leading to $2^n - 1$ using the above sequence as a building block. To do this, we perform a $(s_{i+1} - s_{\sigma(i+1)})$ repeated doubling of the term $2^{s_{\sigma(i+1)}} - 1$ for each $i \in \{0, \ldots, \delta(n) - 1\}$ and include the result of each doubling in the sequence. We claim that this construction yields an addition chain that leads to $2^n - 1$. To see this, we observe

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

for each $0 \leq i \leq \delta(n) - 1$. Here, we observe that the exponent $s_{i+1} - s_{\sigma(i+1)} := s_{\tau(i+1)}$ is a term in the addition chain C_n for $0 \leq i \leq \delta(n) - 1$. The total length of the constructed addition chain is therefore

$$\delta(2^n - 1) = \sum_{i=0}^{\delta(n)-1} s_{\tau(i+1)} + \delta(n).$$

Since the construction holds for any fixed decomposition of terms in the fixed chain C_n in any family $F_{\delta(n),n}$, we deduce

$$\begin{aligned}
\ell(2^n - 1) &\leq \min_{\delta(n)} \left(\min_{F_{\delta(n),n}} \min_{H(C_n)} \left(\sum_{i=0}^{\delta(n)-1} s_{\tau(i+1)} \right) + \delta(n) \right) \\
&= \min_{\delta(n)} \left(\min_{F_{\delta(n),n}} (\mathbb{PV}(C_n)) + \delta(n) \right) \\
&\leq \min_{\delta(n)} \left(\min_{F_{\delta(n),n}} \left(n - 1 + \sum_{i=1}^{\delta(n)-1} (1 - m_i) s_i \right) + \delta(n) \right) \\
&= \min_{\delta(n)} \left(n - 1 + \min_{F_{\delta(n),n}} \left(\sum_{i=1}^{\delta(n)-1} (1 - m_i) s_i \right) + \delta(n) \right) \\
&\leq n - 1 + \min_{F_{\ell(n),n}} \left(\sum_{i=1}^{\ell(n)-1} (1 - m_i) s_i \right) + \ell(n).
\end{aligned}$$

It remains to evaluate the minimum functional on the right side of the inequality. Since every minimum-length addition chain leading to a target is irreducible (by proposition 3.6), the lemma 4.2 implies

$$\min_{F_{\ell(n),n}} \left(\sum_{i=1}^{\ell(n)-1} (1 - m_i) s_i \right) \leq 0.$$

We deduce

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

□

References

1. A. Brauer, *On addition chains*, Bulletin of the American mathematical Society, vol. 45:10, 1939, 736–739.

2. A. Scholz, *253, Jber. Deutsch. Math* Verein. II, vol. 47, 1937, 41–42.

3. W. Hansen, *Zum Scholz-Brauerschen Problem* Journal für die reine und angewandte Mathematik, vol. 202, Walter de Gruyter, Berlin/New York Berlin, New York, 1959, 129-136.

4. N. M. Clift, *Calculating optimal addition chains*, Computing, vol. 91:3, Springer, 2011, 265–284.

5. E. G. Thurber, *The Scholz-Brauer problem on addition chains*, Pacific J. Math., vol. 49:1, Mathematical Sciences Publishers, 1973, 229–242.

6. F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO-Theoretical Informatics and Applications, vol.

24:6, EDP Sciences, 1990, 531–543.

7. P. De Rooij, *Efficient exponentiation using precomputation and vector addition chains*, Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, 389–399.

8. Y. Yacov, *Exponentiating faster with addition chains*, Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1990, 222–229.

9. P. Downey, B. Leong, and R. Sethi, *Computing sequences with addition chains*, SIAM Journal on Computing, vol. 10:3, SIAM, 1981, 638–646.

10. C. T. Whyburn, *A note on addition chains*, Proceedings of the American Mathematical Society, vol. 16, 1965, 1134.

11. W. R. Utz, *A note on the Scholz–Brauer problem in addition chains*, Proceedings of the American Mathematical Society, vol. 4:3, 1953, 462–463.

12. A. Tall, *The Scholz conjecture is true for infinitely many integers with* $\iota(2n) = \iota(n)$, Integers, vol. 24, 2024, p. 2.

13. A. A. Gioia, M. V. Subbarao, and M. Sugunamma, *The Scholz-Brauer problem in addition chains*, 1962.

Departement de mathematiques et de statistique, Universite Laval, Quebec, Canada
E-mail address: thaga1@ulaval.ca/Theophilus@aims.edu.gh/emperordagama@yahoo.com