THE SCHOLZ CONJECTURE ON ADDITION CHAINS IS TRUE FOR INFINITELY MANY INTEGERS WITH $\ell(2n) = \ell(n)$

Amadou Tall
Dept. de Mathématiques et Informatique, Université Cheikh Anta Diop de Dakar, Senegal
amadou7.tall@ucad.edu.sn

Received: 7/2/23, Revised: 8/23/23, Accepted: 12/15/23, Published: 5/27/24

Abstract

We denote by $\ell(n)$ the length of the minimal addition chains for n, and, by $v(n)$ the number of 1's in the binary expansion of n. This paper gives a proof by construction that the Scholz conjecture on addition chains is true for integers of the form $c_1 \cdot 2^{2m+k+3} + c_2$, with $c_1 = 5 \cdot 2^{m+2} + 3$ and $c_2 = 3 \cdot 2^{m+1} + 1$. Such integers satisfy $\ell(n) = \ell(2n)$ and $v(n) = 7$. It is known that the Scholz conjecture on addition chains is true for all integers n with $v(n) \leq 6$. There are no specific results on integers with $v(n) = 7$.

1. Introduction

Let n be a positive integer. The problem of finding a minimal addition chain for n is very interesting. Addition chains can give the fastest exponentiation methods. Finding a good way to reach n from 1 leads to a method of computing x^n.

Definition 1. An *addition chain* for a positive integer n is a set of integers

$$\mathcal{C} = \{a_0 = 1,\ a_1 = 2,\ \ldots,\ a_k,\ \ldots,\ a_r = n\}$$

where every element a_k is written as the sum $a_i + a_j$ of two preceding elements of the set.

Definition 2. Let $\mathcal{C} = \{a_0 = 1,\ a_1,\ a_2 < \ldots,\ a_r = n\}$ be an addition chain for n. Let $a_k = a_i + a_j$ be a step in the chain. If $i = j$, then the step k is called a *doubling step*. Otherwise, it is called a *small step*.

Definition 3. We define $\ell(n)$ as the smallest r for which there exists an addition chain $\{a_0 = 1,\ a_1,\ a_2 < \ldots,\ a_r = n\}$ for n.

DOI: 10.5281/zenodo.11352969

Definition 4. Let n be an integer. We define $v(n)$ as the number of 1's in the binary expansion of n. Let us also define $\lambda(n)$ to be $\lceil \log_2(n) \rceil$.

The problem of finding $\ell(n)$ for a given n is known to be NP–complete. An integer n can also have several distinct minimal addition chains. One of the most efficient methods is the so-called *fast exponentiation* which refers to the binary method. Knuth [11] proved that it is the fastest method for all integers with $v(n) \leq 3$ as stated in the following theorem.

Theorem 1. *Let n be a positive integer. Then the following hold:*

1. *If $n = 2^a$, meaning $v(n) = 1$, then $\ell(n) = a$;*
2. *If $n = 2^a + 2^b$, meaning $v(n) = 2$ with $a > b$, then $\ell(n) = a + 1$;*
3. *If $n = 2^a + 2^b + 2^c$ with $a > b > c$, meaning $v(n) = 3$, then $\ell(n) = a + 2$.*

It becomes interesting to look at techniques based on the binary expansion of n. If $v(n) = 4$, then $n = 2^a + 2^b + 2^c + 2^d$ with $a > b > c > d$ and $\ell(n) \in \{a+2,\ a+3\}$. And it is the same case for $v(n) = 5$ where $\ell(n) \in \{a+3, a+4, a+5\}$. Thurber [14] proved that there are integers with $v(n) \geq 6$ and $\ell(n) = a + 4$. It is difficult to characterize the integers based on their binary representation. N. Clift [3] managed to list all integers having 4 or 5 small steps in their minimal addition chains, meaning $\ell(n) = a + 4$ or $\ell(n) = a + 5$.

The Scholz conjecture gives a bound on the length of minimal addition chains for integers with only 1's in their binary representation. In 1937, the following was stated.

Conjecture 1. Let n be a positive integer. The Scholz conjecture [13] (also called Scholz–Bauer conjecture) on addition chains asserts that:

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

Let us define the notion of *short addition chain*.

Definition 5. Let n be a positive integer, an addition chain for $2^n - 1$ is called a *short addition chain* if its length is $\ell(n) + n - 1$.

Knuth [11] proved that the Scholz conjecture is true for $n \leq 16$. Later, Thurber [15] proved that the same conjecture holds for $n \leq 32$. Aiello et al. [9] proved that it is true for all integers with $v(n) = 1$. It gained interest and has been proven to hold for $v(n) \leq 5$, it is also true for $v(n) = 6$ with $\ell(n) = \lfloor \log_2(n) \rfloor + 3$ and $\ell(n) = \lfloor \log_2(n) \rfloor + 5$, thanks to Hatem [10] and Knuth [11]. No results are known for integers with $v(n) = 7$ and $\ell(n) = \lfloor \log_2(n) \rfloor + 4$.

Now, let us look at the product of integers.

Definition 6. Let c_1 and c_2 be addition chains for n_1 and n_2, respectively. Then $c_1 \times c_2$ is an addition chain for $n_1 \times n_2$ of length $\ell(c_1) + \ell(c_2)$ where $\times$ is defined as follows:

if $c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\}$ and $c_2 = \{b_0,\ b_1,\ \ldots,\ b_l\}$, then

$$c_1 \times c_2 = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r \times b_1,\ a_r \times b_2,\ \ldots,\ a_r \times b_l\}.$$

Definition 7. The above described method to construct an addition chain for n based on its factorization is called the *factor method*.

The length of the new chain is the sum of the length of the chains, meaning that $\ell(mn) \leq \ell(n) + \ell(m)$. We believe that $\ell(2n) = \ell(n) + 1$ and it is easy to prove the following lemma.

Lemma 1. *If the Scholz conjecture is true for n, and $\ell(2n) = \ell(n) + 1$, then it holds for $2n$.*

Proof. Using the factor method,

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

we can deduce a chain for $2^{2n} - 1$ of length

$$\ell(n) + n - 1 + n + 1 = \ell(n) + 2n = \ell(2n) + 2n - 1.$$

The chain is

$$\mathcal{C} = \{1,\ 2,\ \ldots,\ 2^n - 1,\ 2(2^n - 1),\ 2^2(2^n - 1), \ldots,$$

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

□

There exist infinitely many integers with $\ell(2n) \leq \ell(n)$. Thurber [14] has listed a group of integers with $v(n) = 7$, $\ell(n) = \lfloor \log_2(n) \rfloor + 4$ and $\ell(2n) = \ell(n)$. In this paper, we prove that the Scholz conjecture is true for Thurber's list.

2. Preliminary Results

The following results give a method to construct addition chains for $2^n - 1$ based on chains for n.

Lemma 2. *If $n = 2A$ for some A, then we can construct an addition chain for $2^n - 1$ by adding $A + 1$ steps to a chain for $2^A - 1$.*

Proof. If $n = 2A$ for some A, then

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

Using the factor method, we can deduce a chain for $2^n - 1$ with respect to the theorem as follows:

$$\mathcal{C} = \{1,\ 2, \cdots, (2^A - 1),\ 2(2^A - 1),\ 2^2(2^A - 1), \cdots,$$
$$\cdots,\ 2^A(2^A - 1),\ 2^A(2^A - 1) + (2^A - 1) = 2^n - 1\}.$$

□

Lemma 3. *Let $n = A + B$ be an integer with A and B appearing in an addition chain for n ($A > B$). Then, we can construct an addition chain for $2^n - 1$ by adding $B + 1$ steps to a chain for $2^A - 1$ which contains $2^B - 1$.*

Proof. Similarly, if $n = A + B$ for some integers A and B, then

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

and

$$\mathbb{C}_n = \{1, 2, \ldots, 2^B - 1, \ldots, 2^A - 1, 2(2^A - 1), \ldots, 2^B(2^A - 1), n = 2^B(2^A - 1) + (2^B - 1)\}.$$

is an addition chain for $2^n - 1$ based on addition chain for $2^A - 1$ which contains $2^B - 1$. □

Let us illustrate Lemma 3 with an example.

Example 1. Let $n = 11$ and $\mathcal{C} = \{1, 2, 3, 5, 10, 11\}$ be a chain for 11.Using our method, a chain for $2^{11} - 1$ will be constructed as follows:

1. The first element of the chain is 1;
2. since $2 = 2 \times 1$ is in the chain, we will add 2 and $2^2 - 1 = 3 = 2 + 1$;
3. since $3 = 2 + 1$, we need a chain for $2^2 - 1 = 3$ which contains $2^1 - 1 = 1$, we add to the chain $2 \times 3 = 6$ and $2 \times 3 + 1 = 7$;
4. since $5 = 3 + 2$, we need a chain for $2^3 - 1 = 7$ which contains $2^2 - 1 = 3$, we add 2×7, $2^2 \times 7$ and last $2^2 \times 7 + 3 = 31$;
5. since $10 = 5 \times 2$, we will add $2(2^5 - 1) = 62,\ 2^2(2^5 - 1) = 124,\ 2^3(2^5 - 1) = 248,\ 2^4(2^5 - 1) = 496,\ 2^5(2^5 - 1) = 992$ and finally $(2^{10} - 1) = 1023$
6. since $11 = 10 + 1$, we need to add $2(2^{10} - 1)$ and $2(2^{10} - 1) + 1$
7. The chain for $2^{11} - 1$ is then

$$\mathcal{C} = \{1,\ 2,\ 3 = 2^2 - 1,\ 6,\ 7 = 2^3 - 1,\ 14,\ 28,\ 31 = 2^5 - 1,\ 62,\ 124,\ 248,\ 496,\ 992,$$
$$1023 = 2^{10} - 1,\ 2046,\ 2047 = 2^{11} - 1\}.$$

3. Main Results

Let m and k be two positive integers with $k \geq 3$. Let $c_1 = (101\underbrace{0\cdots0}_{m}11)_2 = 5 \cdot 2^{m+2}+3$ and $c_2 = (11\underbrace{0\cdots0}_{m}1)_2 = 3\cdot 2^{m+1}+1$ be two integers. The following lemmas will be used to prove that the Scholz conjecture is true for $n = c_1 \cdot 2^{2m+k+3} + c_2$ and $2n$.

Lemma 4. *We can construct an addition chain for c_1 of length $m+7$ which contains c_2, knowing that*

$$\ell(c_1) = m+6, \quad \textit{and} \quad \ell(c_2) = m+4.$$

Proof. It is easy to see that $v(c_1) = 4$ and $v(c_2) = 3$. Knuth [11] proved that $\ell(c_1) = \lambda(c_1) + 2 = m+6$. Similarly for c_2.

An addition chain for $c_1 = 3c_2 + 2^{m+1}$ is

$$\mathcal{C} = \{1,\ 2,\ \ldots,\ 2^{m+1},\ 2\cdot 2^{m+1},\ 3\cdot 2^{m+1},\ c_2,\ 2c_2,\ 3c_2 = 2c_2 + c_2,\ 3c_2 + 2^{m+1}\}$$

and $\ell(\mathcal{C}) = m+7$. □

Lemma 5. *We can construct a chain for $2^{c_1}-1$, having length $\ell(c_1)+c_1 = c_1+m+6$, that contains $2^{c_2}-1$.*

Proof. We know that $c_1 = 3c_2 + 2^{m+1}$, so

$$\begin{aligned}
2^{c_1} - 1 &= 2^{3c_2+2^{m+1}} - 1,\\
&= 2^{2^{m+1}}(2^{3c_2} - 1) + (2^{2^{m+1}} - 1),\\
&= 2^{2^{m+1}}(2^{c_2}(2^{2c_2} - 1) + (2^{c_2} - 1)) + (2^{2^{m+1}} - 1),\\
&= 2^{2^{m+1}}(2^{c_2}((2^{c_2} - 1)(2^{c_2} + 1)) + (2^{c_2} - 1)) + (2^{2^{m+1}} - 1).
\end{aligned}$$

Then, we can construct a chain for $2^{c_1}-1$ which contains $2^{c_2}-1$ and $2^{2^{m+1}}-1$ as follows:

1. Start by a chain for $2^{c_2}-1$ which contains $2^{2^{m+1}}-1$ using the chain c_2.
2. Use the factor method to get the chain for $(2^{c_2}-1)(2^{c_2}-1) = 2^{2c_2}-1$.
3. Add c_2 doubling to get $2^{c_2}(2^{2c_2}-1) = 2^{3c_2}-1$.
4. Add 2^{m+1} doubling to reach $2^{2^{m+1}}(2^{3c_2}-1)$.
5. Add $2^{2^{m+1}}-1$.

The total length is $\ell(2^{c_2}-1) + c_2 + (c_2+1) + 1 + 2^{m+1} + 1 = c_1 + m + 6$. □

The following theorems prove that the Scholz conjecture is true for Thurber's list.

Theorem 2. *Let m and k be positive integers with $k \geq 3$. The Scholz conjecture on addition chains is true for all integers of the form*

$$n = (101\underbrace{0\cdots0}_{m}11\underbrace{0\cdots0}_{k}11\underbrace{0\cdots0}_{m}1)_2 = c_1 \cdot 2^{2m+k+3} + c_2.$$

Proof. We know that

$$\begin{aligned} 2^n - 1 &= 2^{c_1 \cdot 2^{2m+k+3}+c_2} - 1, \\ &= 2^{c_2}(2^{c_1 \cdot 2^{2m+k+3}} - 1) + (2^{c_2} - 1), \\ &= 2^{c_2}((2^{c_1} - 1)(2^{c_1} + 1)(2^{2c_1} + 1)(2^{2^2 c_1} + 1) \cdots (2^{2^{2m+k+2} c_1} + 1)) + (2^{c_2} - 1). \end{aligned}$$

And we have a chain for $2^{c_1} - 1$ which contains $2^{c_2} - 1$. The following is an addition chain for $2^n - 1$:

$$\mathcal{C} = \{1,\ 2,\ \ldots,\ (2^{c_2} - 1), \ldots, (2^{c_1} - 1),\ \ldots,\ (2^{2c_1} - 1) = (2^{c_1} - 1)(2^{c_1} + 1),$$

$$\ldots,\ (2^{2^{2m+k+3} c_1} - 1),\ 2(2^{2^{2m+k+3} c_1} - 1),\ \ldots,\ 2^{c_2}(2^{2^{2m+k+3} c_1} - 1),\ n\}.$$

Its length is

$$(c_1 + m + 6) + c_2 + (2m + k + 3) + c_1(2^{1m+k+3} - 1) + 1 = n + 2m + k + 10 = \ell(n) + n - 1.$$

Some details follow below:

1. $c_1 + 1$ steps to go from $2^{c_1} - 1$ to $2^{2^2 c_1} - 1 = (2^{c_1} - 1)(2^{c_1} + 1)$;

2. $2c_1 + 1$ steps to go from $2^{2c_1} - 1$ to $2^{2^2 c_1} - 1 = (2^{2c_1} - 1)(2^{2c_1} + 1)$;

3. $2^2 c_1 + 1$ steps to go from $2^{2c_1} - 1$ to $2^{2^{2^2} c_1} - 1 = (2^{2^2 c_1} - 1)(2^{2^2 c_1} + 1)$;

4. and so on;

5. $2^{2m+k+2} c_1 + 1$ steps to go from $2^{2^{2m+k+2} c_1} - 1$ to $2^{2^{2m+k+3} c_1} - 1 = (2^{2^{2m+k+2} c_1} - 1)(2^{2^{2m+k+2} c_1} + 1)$.

□

Our next result states that the Scholz conjecture is also true for $2n$.

Theorem 3. *Let n be defined as in the previous theorem. The Scholz conjecture on addition chains is true for $2n$.*

Proof. Let c_3 and c_4 denote $(2^{m+4}+2^{m+2}+2+1)$ and $2^{m+3}+2^{m+2}+2$, respectively. A minimal addition chain for c_3 which contains c_4 is

$$\mathcal{C} = \{1,\ 2, \ldots,\ 2^{m+2},\ ,\ 2^{m+2}+1, ,\ 2^{m+3}+1, ,\ 2^{m+3}+2^{m+2}+2,\ 2^{m+4}.+2^{m+2}+2+1\}$$

$\mathcal{C}$ is a short addition chain for $2^{c_3}-1$ which contains $2^{c_4}-1$.

On the other hand,

$$2n = (2^{m+4}+2^{m+2}+2+1)\cdot(2^{m+k+4}) + (2^{m+3}+2^{m+2}+2)$$

, and we can construct an addition chain for $2^{2n}-1$ using the following expression,

$$\begin{aligned}
2^{2n}-1 &= 2^{(2^{m+4}+2^{m+2}+2+1)\cdot(2^{m+k+4})+(2^{m+3}+2^{m+2}+2)} - 1, \\
&= 2^{c_3\cdot(2^{m+k+4})+c_4} - 1, \\
&= 2^{c_4}(2^{c_3\cdot(2^{m+k+4})} - 1) + (2^{c_4}-1), \\
&= 2^{c_4}((2^{c_3}-1)(2^{c_3}+1)(2^{2c_3}+1)\cdots((2^{2^{m+k+3}c_3}+1))) + (2^{c_4}-1).
\end{aligned}$$

Similar techniques are applied to get an addition chain for $2^{2n}-1$ of length $(\ell(c_3)+c_3-1)+c_4+(m+k+4)+c_3(2^{m+k+4}-1) = 2n+2m+k+10 = \ell(2n)+2n-1$. $\square$

Theorem 4. *The Scholz conjecture on addition chains is true for infinitely many integers n with $\ell(2n) = \ell(n)$.*

Proof. Let m and k be positive integers with $k \geq 3$.

Let $n = 101\underbrace{0\cdots0}_{m}11\underbrace{0\cdots0}_{k}11\underbrace{0\cdots0}_{m}1$ be a positive integer. We have proven that the Scholz conjecture is true for both n and $2n$. $\square$

4. Conclusion

In this paper, we have proven that the Scholz conjecture on addition chains is true for infinitely many integers n. It is still unproven to hold for all integers n with $\ell(2n) = \ell(n)$. More generally, if the Scholz conjecture is true for n, one can investigate its behavior on mn knowing that there are infinitely many integers with $\ell(mn) \leq \ell(m)$.

Acknowledgments. The author would like to express his special thanks to the referees for their useful comments. He would like to extend his thanks to the staff of IHES. He is particularly grateful to Mike Bennett for the joyful discussions they had at UBC. This work is partially supported by the Simons Foundation.

References

[1] F. Achim, http://www.homes.uni-bielefeld.de/achim/addition_chain.html.

[2] J.J Bravo, B. Faye, F. Luca and A. Tall, Repdigits as Euler functions of Lucas numbers, *An. Stiint. Univ. Ovidius Constanta Ser. Mat.* **24** (2) (2016), 105-126.

[3] N. M. Clift, http://additionchains.com/.

[4] N. M. Clift, Calculating optimal addition chains, *Computing* **91** (3) (2011), 265-284.

[5] B. Edjeou, A. Tall and M. B. Fraj Ben-Maaouia, Powers of two as sums of three Lucas numbers, *J. Integer Seq.* **23** (2020), Article 20.8.8.

[6] B. Edjeou, A. Tall and M. B. Fraj Ben Maaouia, On pillai's problem with Lucas numbers and powers of 3, *Integers* **21** (2021), #A108.

[7] B. Faye, M. D. Taoufiq, F. Luca and A. Tall, Fibonacci numbers with prime sums of complementary divisors, *Integers* **14** (2014), #A5.

[8] B. Faye, M. D. Taoufiq, F. Luca and A. Tall, Members of Lucas sequences whose Euler function is a power of 2, *Fibonacci Quart.* **52** (1) (2014), 3-9.

[9] A. A. Gioia, M. V. Subbarao and M. Sugunamma, The Scholz-Brauer problem in addition chains, *Duke Math. J.* **29** (1962), 481-487.

[10] H. M. Bahig and K. Nakamula, Some properties of nonstar steps in addition chains and new cases where the Scholz conjecture is true, *J. Algorithms* **42** (2) (2002), 304-316.

[11] D.E. Knuth, *The Art of Computer Programming, Volume 2*, Addison-Wesley, MA, 1969.

[12] M. Mignotte and A. Tall, A note on addition chains, *Internat. J. Algebra* **5** (6) (2011), 269 - 274.

[13] A. Schönhage, A lower bound for the length of addition chains, *Theoretical Computer Science* **1**(1975) 1-12.

[14] E. G. Thurber, Addition chains and solutions of $\ell(2n) = \ell(n)$ and $\ell(2^n - 1) = \ell(n) + n - 1$, *Discrete Math.* **16** (1976) 279-289.

[15] E. G. Thurber, The Scholz-Brauer problem on addition chains, *Pacific J. Math.* **49** (1) (1973) 229-242.

[16] E. G. Thurber and N. M. Clift, Addition chains, vector chains, and efficient computation, *Discrete Math.* **344** (2) (2021) 112200