# The Scholz conjecture on addition chain is true for $v(n) = 4$

Amadou TALL[1]

Departement de Mathématiques et Informatique
Université Cheikh Anta Diop de Dakar
amadou7.tall@ucad.edu.sn

**Abstract.** The aim of this paper is to prove that the Scholz conjecture on addition chain is true for all integers with $v(n) = 4$, $v(n)$ is the number of "1" in the binary expansion of $n$.

## 1 Introduction

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

$$\mathcal{C} = \{a_0 = 1, a_1, a_2, \ldots, a_r = n\}$$

*such that*

$$\forall k \in [2..r], \exists i, j \in [1..k-1], \quad a_k = a_i + a_j$$

*and $a_r = n$.*

The integer $r$ is the length of the chain $\mathcal{C}$ and can be denoted $\ell(\mathcal{C})$.

**Definition 2.** *We define $l(n)$ as the smallest $r$ for which there exists an addition chain $\{a_0 = 1, a_1, a_2, \ldots, a_r = n\}$ for $n$.*

There exist several methods to compute an addition chain for any integer $n$. We can cite the binary method (often called the fast exponentiation method), the m-ary method, the factor method to name a few. However, the problem of finding $\ell(n)$ for a given $n$ is known to be NP–complete.

A first attempt were done based on the binary expansion of integers.

**Definition 3.** *Let $n$ be an integer. The number of "1"s in its binary expansion is called the Hamming weight of $n$ and is denoted $v(n)$.*

It has been proven that

**Theorem 4.**

$$\ell(n) = a + v(n) - 1 \quad \forall v(n) \leq 3,$$

meaning that $\ell(2^a) = a$, $\ell(2^a + 2^b) = a + 1$, and $\ell(2^a + 2^b + 2^c) = a + 2$. The case where $v(n) = 4$ have some particularities as follows

**Theorem 5.** *For all integers $n$ such that $n = 2^a + 2^b + 2^c + 2^d$, we have*

$$\ell(n) = a + 3,$$

*except for the integers satisfying one of the following conditions, where $\ell(n) = a + 2$*

1. $a - b = c - d$
2. $a - b = c - d + 1$
3. $a - b = 3$ *and* $c - d = 1$
4. $a - b = 5$ *and* $b - c = c - d = 1$

More informations can be found in Knuth [1]. They can be proven using the binary method which is based on the Hamming weight. We are now concerned about integers with only "1"s in their binary expansion ($2^n - 1$). Is the binary method still efficient? The answer is no. Scholz conjectured that we can always find an addition chain for $2^n - 1$ of length $\leq \ell(n) + n - 1$.

**Definition 6.** *Let $n$ be a positive integer, an addition chain for $2^n - 1$ is called a short addition chain if its length is $\ell(n) + n - 1$.*

The most famous conjecture on addition chains is the Scholz's conjecture stating that

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

Aiello and Subbarao [5] have conjectured that for every integer $n$, there exist a short addition chain for $2^n - 1$ (an addition chain for $2^n - 1$ of lenght $\ell(n) + n - 1$).

$$\forall n \in \mathbb{N},\ \exists \text{ an addition chain for } 2^n - 1 \text{ of length } \ell(n) + n - 1$$

They have shown that it is true for all $n = 2^k$.

**Theorem 7.** *It's known that*

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

*And we know a way of computing such chains.*

We can see that a short addition chain is not necessarily a minimal addition chain but, finding a short addition chain for $2^n - 1$ is enought to prove that the Scholz-Brauer conjecture is true for $n$.

The main result of this paper is the proof that:

$$v(n) \leq 4 \Rightarrow \ell(2^n - 1) \leq \ell(n) + n - 1.$$

We will conduct a proof by induction on the Hamming weight of integers. It will then be used to get an algorithm for the computation of short addition chains for $2^n - 1$.
Our proof will be using the factoring method which can be stated as follows

**Definition 8.** *Let $\mathcal{C}_\backslash$ and $\mathcal{C}_\Updownarrow$ be respectively two addition chains for $n$ and $m$. The factor method is a method to obtain an addition chain $\mathcal{C}_{\Updownarrow\backslash}$ for $mn$ as follows:*
*If*

$$\mathcal{C}_\Updownarrow = \{m_0, m_1, \ldots, m_r\}$$

*and*

$$\mathcal{C}_\backslash = \{n_0, n_1, \ldots, n_t\}$$

*then*

$$\mathcal{C}_{\Updownarrow\backslash} = \{a_0, a_1, \ldots, a_r, a_{r+1}, a_{r+2}, \ldots, a_{r+t}\}$$

*with $a_i = m_i \forall i \leq r$ and $a_{r+i} = m_r \times n_i$.*

On can clearly see that $\mathcal{C}_{\Updownarrow\backslash}$ is an addition chain and $a_{r+t} = m_r \times n_t = mn$.
and we have a clear idea on the lenght of the chain

**Theorem 9.**

$$\ell(mn) \leq \ell(m) + \ell(n)$$

The proof is simple, one can easily construct an addition chain for $mn$ based on the chains for $m$ and $n$.

## 2 Main results

Here is the first result of this paper.

**Theorem 10.** *For all integers $n = 2^k + 2^i$, with $i < k$, we can find a short chain for $2^n - 1$. Which implies that*

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

*Proof.* Let

$$P_k = \{\text{we have a short addition chain for } 2^n - 1, \text{ where } n = 2^k + 2^i, \text{ with } i < k\}.$$

Clearly, $P_1 = \{$we have a short addition chain for $3\}$ is true.
We assume that $P_k$ is true for all $k < k_0$ and let $n = 2^{k_0} + 2^i$ for some $i$.

**First case:** $i > 0$

We have the relation

$$2^n - 1 = 2^{2^{k_0}+2^i} - 1 = (2^{2^{k_0-1}+2^{i-1}} - 1)(2^{2^{k_0-1}+2^{i-1}} + 1).$$

And we do know that:

**(i)** A minimal addition chain for $2^{2^{k_0-1}+2^{i-1}} + 1$ is given by the binary method and has length $2^{k_0-1} + 2^{i-1} + 1$.
**(ii)** Thanks to $P_{k_0-1}$, we have a chain of length $2^{k_0-1} + 2^{i-1} + k_0 - 1$ for the integer $2^{2^{k_0-1}+2^{i-1}} - 1$.

Using the factor method, we have a chain for $2^n - 1$ of length:

$$(2^{k_0-1} + 2^{i-1} + 1) + (2^{k_0-1} + 2^{i-1} + k_0 - 1) = 2^{k_0} + 2^i + k_0,$$

and the result holds in this case.

**Second case:** $i = 0$

Then

$$2^n - 1 = 2^{2^{k_0}+1} - 1 = 2(2^{2^{k_0}} - 1) + 1.$$

And we do know that:

**(i)** An addition chain for $2^{2^{k_0}} - 1$ of length $2^{k_0} + k_0 - 1$ is given by [5].
**(ii)** We need two star steps more to reach $2^n - 1$, a doubling and a "+1".

We deduce that we have a chain of length $2^{k_0} + k_0 + 1$ for $2^n - 1$.
This ends the proof of the result.

Now let us state the second result of this paper.

**Theorem 11.** *For all integers $n = 2^k + 2^i + 2^j$, we have*

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

*and we can find short addition chain for $2^n - 1$.*

*Proof.* Let

$$P_k = \{\exists \text{ an addition chain for } 2^n - 1 \text{ of length } \ell(n) + n - 1, \text{ where } n = 2^k + 2^i + 2^j, \text{ with } k > i > j\}.$$

We know that $P_3$ is true. And we have proved above that $P_2$ is also true.
Suppose that $P_k$ is true for all $k < k_0$. Then, let $n = 2^{n_1} + 2^{n_2} + \cdots + 2^{n_{k_0}}$ be an integer of Hamming weight $k_0$.

**First case:** $j = 0$

We can write

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

We know that $v(n-1) = 2$, the previous result shows that we can find an addition chain for $2^{n-1} - 1$ of length

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

Adding the two last star steps to reach $2^n - 1$, we obtain—as wanted—a chain of length

$$\begin{aligned}(\ell(n-1) + (n-1) - 1) + 2 &= \ell(n-1) + (n-1) + 1, \\ &= (k+1) + (2^k + 2^j) + 1, \\ &= 2^k + 2^j + k + 2.\end{aligned}$$

**Second case** $j > 0$

In this case

$$n = 2^k + 2^i + 2^j = 2(2^{k-1} + 2^{i-1} + 2^{j-1}).$$

So, we can write

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

We know that

**(i)** a minimal addition chain for $2^{\frac{n}{2}} + 1$ of length $\frac{n}{2} + 1$ is given by the binary method,
**(ii)** $P_{k_0 - 1}$ is true, thus we have a short addition chain for $2^{\frac{n}{2}} - 1$, its length is equal to $\ell(\frac{n}{2}) + \frac{n}{2} - 1$.

Using the factor method, we have an addition chain for $2^n - 1$ of length

$$\Big(\frac{n}{2} + 1\Big) + \Big(\ell(\frac{n}{2}) + \frac{n}{2} - 1\Big) = \ell(n/2) + n.$$

By adding one star step to a minimal chain for $\frac{n}{2}$, we obtain a chain for $n$. Then, we have found a chain for $2^n - 1$ of length $\ell(n) + n - 1$.

Here is the third and most interesting case ($v(n) = 4$). There will be two cases. The first is when $\ell(n) = a+3$ and the proof will be identical to the above ones. And the second case is when $\ell(n) = a+2$ and we know all the four possibilities of $n$.

**Theorem 12.** *If* $n = 2^a + 2^b + 2^c + 2^d$ *and* $\ell(n) = a + 3$*, then we can construct a short addition chain for* $n$*.*

The proof for the case where $\ell(n) = a + 3$ is identical to the above proof, one can easily prove it using the induction way presented above.

*Proof.* 1. $d = 0$

In this case $\ell(n-1) = a + 2$, and we have

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

We also know that

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

then we can reach $n$ by adding two step to a chain for $2^{n-1} - 1$ of lenght $\ell(n-1) + n - 1$, so

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

2. $d > 0$

we have

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

using the factor method, we have an addition chain for $2^n - 1$ of lenght

$$\begin{aligned} (\frac{n}{2} + 1) + (\frac{n}{2^2} + 1) + \cdots + (\frac{n}{2^d} + 1) + \ell(\frac{n}{2^d}) + \frac{n}{2^d} - 1, \\ = (\frac{n}{2} + \frac{n}{2^2} + \cdots + \frac{n}{2^d} + \frac{n}{2^d}) + d + \ell(\frac{n}{2^d}) - 1, \\ = \ell(n) + n - 1. \end{aligned} \tag{1}$$

and this gives us the result

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

thanks to the fact that $2^{\frac{n}{2^d}} - 1$ satisfies the case 1.

The remaining case is:

**Theorem 13.** *If* $n = 2^a + 2^b + 2^c + 1$ *and* $\ell(n) = a + 2$*, then we can construct a short addition chain for* $n$*.*

*Proof.* Let $n = 2^a + 2^b + 2^c + 1$ and $\ell(n) = a + 2$ then $n$ is in one of these four cases,

1. $n = 2^a + 2^b + 2^c + 1$ with $a - b = c$, we can write

$$n = 2^b(2^{a-b} + 1) + 2^c + 1 = (2^b + 1)(2^c + 1).$$

and that give us a simple way of reaching $2^n - 1$

$$\begin{aligned} 2^n - 1 &= 2^{(2^b+1)(2^c+1)} - 1 \\ &= 2^{2^c+1}(2^{(2^c+1).2^b} - 1) + 2^{2^c+1} - 1 \end{aligned}$$

and we can also write $2^n - 1$ this way,

$$2^{2^c+1}\{(2^{2^c+1} - 1)(2^{(2^c+1)} + 1)(2^{(2^c+1)\cdot 2} + 1)(2^{(2^c+1)\cdot 2^2} + 1)\cdots(2^{(2^c+1)\cdot 2^{b-1}} + 1)\} + 2^{2^c+1} + 1$$

using the factor method, we can now have an addition chain for $2^n - 1$ of lenght

$$\ell(2^c - 1) + 2^c + 1 - 1 + 2^c + 1 + 1 + b + (2^c + 1)(1 + 2 + 2^2 + \cdots + 2^{b-1})$$

after some rearrangements, we can see that the above value is

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

2. $n = 2^a + 2^b + 2^c + 1$ with $a - b = c + 1$,
We have

$$n = 2^a + 2^b + 2^c + 1 = 2^b(2^{c+1} + 1) + (2^c + 1)$$

which allows to write

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

which gives

$$2^n - 1 = 2^{2^c+1}((2^{2^{c+1}+1} - 1)(2^{2^{c+1}+1} + 1)(2^{2(2^{c+1}+1)} + 1)(2^{2^2(2^{c+1}+1)} + 1)\ldots(2^{2^{b-1}(2^{c+1}+1)} + 1)) + (2^{2^c+1} - 1)$$

It leads to an addition chain of length

$$\ell() + (2^c + 1) + (2^{c+1} + 1 + 1) + (2(2^{c+1} + 1) + 1) + \ldots + (2^{b-1}(2^{c+1} + 1) + 1) + 2^c + 1 + 1$$

after regrouping, we get that the lenght is

$$\ell(2^c + 1) + 2^c + 1 - 1 + 2^c + 1 + b + (2^{c+1} + 1)(1 + 2 + \cdots + 2^{b-1}) + 2^c + 1 + 1 =$$

$$= c + 1 + 2^c + 2^c + 1 + b + (2^{c+1} + 1)(2^b - 1) + 2^c + 2 = 2^{b+c+1} + 2^b + 2^c + b + c + 3 = \ell(n) + n - 1.$$

3. $n = 2^a + 2^b + 2^c + 1$ with $a - b = 3$ and $c = 1$, we can see that

$$n = 3 + 2^b(1 + 2^3) = 3 + 9 \cdot 2^b,$$

and we can get now $2^n - 1$ this way

$$2^n - 1 = 2^{3+9\cdot 2^b} - 1 = 2^3(2^{9\cdot 2^b} - 1) + 2^3 - 1.$$

Knowing that a short addition chain for $2^{9\cdot 2^b} - 1$ that contains $2^3 - 1$ is obtained by the way describe above, we can again use the factor method to get an addition chain for $2^n - 1$ of length

$$\ell(2^{9\cdot 2^b} - 1) + 3 + 1 = \ell(9 \cdot 2^b) + 9 \cdot 2^b - 1 + 3 + 1 = n + \ell(n) - 1.$$

4. $n = 2^a + 2^b + 2^c + 1$ with $a - b = 5,\ b - c = c = 1$ , then

$$n = 2^7 + 2^2 +^2 +1 = 135,$$

and we already know that the conjecture is true for this one. We already have a short addition chain for $2^{135} - 1$.

**Theorem 14.** *If $n = 2^a + 2^b + 2^c + 2^d$ with $d > 0$ and $\ell(n) = a + 2$, then we can construct a short addition chain for $n$.*

*Proof.*
$$n = 2^a + 2^b + 2^c + 2^d = 2^d \cdot (2^{a-d} + 2^{b-d} + 2^{c-d} + 1)$$
by the first case, we can have a short addition chain for $2^\alpha - 1 = 2^{2^{a-d}+2^{b-d}+2^{c-d}+1} - 1$ of length $\alpha + a - d + 1$.
Since $n = 2^d \cdot \alpha$, then
$$2^n - 1 = 2^{2^d \cdot \alpha} - 1 = (2^\alpha - 1)(2^\alpha + 1)(2^{\alpha \cdot 2} + 1) \cdots (2^{\alpha \cdot 2^{d-1}} + 1)$$
and using the factor method again, we have a chain for $2^n - 1$ of length
$$\alpha + a - d + 1 + \alpha(1 + 2 + 2^2 + \cdots + 2^{d-1}) + d = 2^d\alpha + a - 1 = \ell(n) + n - 1.$$

## Acknowledgments

The author acknowledge the support of IMU throught the Simons foundation. The work was started during a visit at the University of British Columbia. The last part were done during a visit at IHES.

## References

1. D.E. Knuth, *The Art ef Computer Programming*, Vol. 2 (Addison-Wesley, Read. Mass., 1969) 398-422.
2. Maurice Mignotte, Amadou Tall, *A note on addition chains.* International Journal of Algebra, xxx
3. Thurber, Edward G., *The Scholz-Brauer problem on addition chains*, Pacific Journal of Mathematics, V.49 No.1, 1973 p.229-242
4. Schönhage, A. *A Lower Bound for the Length of Addition Chains*, Theoretical Computer Science, V. 1 1975 p. 1-12.
5. A. A. Gioia, M. V. Subbarao, and M. Sugunamma, *The Scholz-Brauer problem in addition chains*, Duke Math. J. 29 (1962), 481-487.