Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2022, Volume 28, Number 2, Pages 276–280
DOI: 10.7546/nntdm.2022.28.2.276-280

A note on the Aiello–Subbarao conjecture on addition chains

Hatem M. Bahig

Department of Mathematics, Faculty of Science,
Ain Shams University Cairo, Egypt
e-mails: hmbahig@sci.asu.edu.eg, h.m.bahig@gmail.com

Received: 21 January 2021 **Revised:** 14 April 2022
Accepted: 9 May 2022 **Online First:** 10 May 2022

Abstract: Given a positive integer x, an addition chain for x is an increasing sequence of positive integers $1 = c_0, c_1, \ldots, c_n = x$ such that for each $1 \leq k \leq n$, $c_k = c_i + c_j$ for some $0 \leq i \leq j \leq k-1$. In 1937, Scholz conjectured that*for each positive integer x,* $\ell(2^x-1) \leq \ell(x)+x-1$, where $\ell(x)$ denotes the minimal length of an addition chain for x. In 1993, Aiello and Subbarao stated the apparently stronger conjecture that *there is an addition chain for* $2^x - 1$ *with length equals to* $\ell(x) + x - 1$. We note that the Aiello–Subbarao conjecture is not stronger than the Scholz (also called the Scholz–Brauer) conjecture.

Keywords: Addition chain, Aiello–Subbarao's conjecture, Scholz–Brauer's conjecture.
2020 Mathematics Subject Classification: 11Y16, 11Y55.

1 Introduction

Given a positive integer x, an *addition chain* [9, 11] for x, denoted by $AC(x)$, is an increasing sequence of positive integers $1 = c_0, c_1, \cdots, c_n = x$ such that

$$\forall\, 1 \leq k \leq n, c_k = c_i + c_j \text{ with some } 0 \leq i \leq j \leq k-1. \tag{1}$$

The length of the chain is n. The minimal value of n for any $AC(x)$ is denoted by $\ell(x)$.

Flammenkamp [6] added another condition on addition chains to ensure that addition chains do not contain superfluous elements. The condition is the following:

$$\forall\, 0 \leq k \leq n-1,\ \exists j \text{ with } k < j \leq n \text{ and } \exists i < j \text{ such that } c_j = c_k + c_i. \tag{2}$$

It is clear that there is a difference between the two definitions. For example, the sequence

$$1, 2, 4, 8, 9, 16$$

is an $AC(16)$ according to the first definition, Eq. (1), while it is not an $AC(16)$ according to the second definition, Eq. (2), since $c_4 = 9$ is not used to construct c_k for any $k > 4$.

Scholz [10, 11] conjectured that for each positive integer x,

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

The Scholz conjecture is usually called the Scholz–Brauer conjecture [8, 12, 13] (simply **S–B** conjecture). The **S–B** conjecture holds when $\omega(x) \leq 5$, where $\omega(x)$ denotes how many 1's in the binary representation of x, [2, 8, 9]. It is also known that the **S–B** conjecture is true if the shortest addition chain is a *Hansen* chain, where a chain is called Hansen's if there is a subset H of members of the chain such that each member of the chain uses the largest element of H which is less than the member, [9]. Let $\ell^0(x)$ denote the length of the shortest Hansen chains. Clearly, $\ell(x) \leq \ell^0(x)$. In [2], the authors pointed out that $\ell(x)$ may be less than $\ell^0(x)$ when, for example, all shortest addition chains for x have an element $c_i = c_j + c_k, j, k \leq i - 3$. Clift [5] found the first number $x = 5784689$, with $\ell(x) < \ell^0(x)$. Therefore, computationally, the **S–B** conjecture holds for all positive integer $x < 5784689$, [3–5, 7].

In order to prove the **S–B** conjecture, Aiello and Subbarao [1] conjectured that there is an $AC(2^x - 1)$ whose length equals $\ell(x) + x - 1$. They proved it for all $x \leq 128$ and for x with $\omega(x) = 1$.

Remark 2.2 of [1] states that the Aiello–Subbarao conjecture (or simply **A–S** conjecture) is stronger than the **S–B** conjecture.

In this paper, we note that the **A–S** conjecture is not stronger than the **S–B** conjecture under the two definitions.

2 The result

In this section, we show that the **A–S** conjecture is not stronger than the **S–B** conjecture. We have two definitions in literature:

The first definition (Eq. (1)): The **A–S** conjecture is not stronger than the **S–B** conjecture since any chain of length n ($\ell(x) \leq n < x - 1$) could be extended to the desired length by blowing it up with an arbitrary positive integer. For example, if we have an $AC(x)$ of length n:

$$1 = c_0, c_1, \ldots, c_n = x,$$

then we can extend it to a chain of length $n + 1$ for x as follows:

$$1 = c_0, c_1, \ldots, c_k, c_k + 1, c_{k+1}, \ldots, c_n = x.$$

In the first addition chain c_k satisfies that $c_{k+1} - c_k > 1$ and $1 \leq k < n$. Clearly such c_k exists since $k < x - 1$.

The second definition (Eq. (2)): Although Flammenkamp's definition was published after the posting of the **A–S** conjecture, we note that Flammenkamp's extra condition on addition chains does not change the result.

Suppose that $c_0, c_1, \ldots, c_n = x$ ($n < x - 1$) is an $AC(x)$ that satisfies Flammenkamp's condition Eq. (2). To construct a new chain of length $n + 1$ for x, we complete two steps:

1. Since $n < x - 1$, find the smallest c_k such that $c_{k+1} - c_k > 1$.
2. Insert the new element $c_k + 1$ between c_k and c_{k+1}.

The new chain is

$$1, 2, 3, 4, \ldots, c_{k-1} = c_k - 1 = k, c_k = k + 1, c_k + 1 = k + 2, c_{k+1}, \ldots, c_n = x.$$

Since $c_{k+1} - c_k > 1$ in the first addition chain, c_{k+1} can be written as the sum $c_k + c_j$, where $c_j \geq 2$. In the new addition chain,

$$c_{k+1} = (c_k + 1) + (c_j - 1) = (c_k + 1) + c_{j-1}.$$

All other elements in the new addition chain are formed as before.

It should be noted that in both cases the process can be repeated if necessary. Therefore, if we have an $AC(2^x - 1)$ with length $n < \ell(x) + x - 1$, then it can be extended to a chain for $2^x - 1$ with length $\ell(x) + x - 1$. Thus, the **A–S** conjecture is not stronger than the **S–B** conjecture.

Now, let us define the following: An $AC(x) : c_0 < c_1 < \cdots < c_n = x$ is called *irredundant*, if no proper subset of $\{c_0, c_1, \ldots, c_n\}$ forms an $AC(x)$. So a proper rephrasing of the **A–S** conjecture would be: *For every positive integer x, the integer $2^x - 1$ has an irredundant addition chain of length $\ell(x) + x - 1$.*

For example, the sequences

$$1, 2, 3, 5, 10, 15$$

and

$$1, 2, 4, 5, 10, 15$$

are two irredundant chains for 15. If we remove any element in the sequences, then the sequences are not addition chains. For examples, if we remove 3 from the first sequence (or 4 from the second sequence), then we cannot write 5 as a sum of two preceding elements. Similarly, if we remove 5 from both sequences, then we cannot write 10 as a sum of two preceding elements.

On the other hand, the sequence $1, 2, 3, 4, 5, 10, 15$ is an $AC(15)$ according to the first and second definitions of addition chains, Eq. (1) and Eq. (2), respectively. Table 1 shows why the sequence is an $AC(15)$ according to Eq. (2). But the sequence is not an irredundant chain since the subsequence $1, 2, 4, 5, 10, 15$ is a proper subset of the given sequence and forms an $AC(15)$, where $2 = 1 + 1, 4 = 2 + 2, 5 = 4 + 1, 10 = 5 + 5, 15 = 10 + 5$.

Similarly, the sequence $1, 2, 4, 5, 8, 10, 18$ is an $AC(18)$ according to the second definition of addition chains, Eq. (2), while it is not irredundant since $1, 2, 4, 8, 10, 18$ is an $AC(18)$.

k	j	i $c_j = c_k + c_i$
0	1	0 $c_1 = c_0 + c_0 = 1 + 1$
1	2	0 $c_2 = c_1 + c_0 = 2 + 1$
2	3	0 $c_3 = c_2 + c_0 = 3 + 1$
3	4	0 $c_4 = c_3 + c_0 = 4 + 1$
4	5	4 $c_5 = c_4 + c_4 = 5 + 5$
5	6	4 $c_6 = c_5 + c_4 = 10 + 5$

Table 1. The sequence $1, 2, 3, 4, 5, 10, 15$ is an $AC(15)$ according to the second definition, Eq. (2).

Open problem: *Is this variation of the* ***A–S*** *conjecture stronger than the* ***S–B*** *conjecture?*

It is observed that an irredundant chain is not necessarily the shortest one. For example, the chain $1, 2, 4, 5, 9, 14, 15$ is irredundant but not the shortest one; see the above examples. On the other hand, any shortest addition chain must be irredundant.

3 Conclusion

We have shown that the **A–S** conjecture is not stronger than the **S–B** conjecture.

Acknowledgements

The author is grateful to the anonymous referees for valuable comments.

References

[1] Aiello, W., & Subbarao, M. V. (1993). A conjecture in addition chains related to Scholz's conjecture. *Mathematics of Computation*, 61(203), 17–23.

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

[3] Bahig, H. M. (2006). Improved generation of minimal addition chains. *Computing*, 78, 161–172.

[4] Bahig, H. M. (2011). Star reduction among minimal length addition chains. *Computing*, 91, 335–352.

[5] Clift, N. M. (2011). Calculating optimal addition chains. *Computing*, 91, 265–284.

[6] Flammenkamp, A. (1999). Integers with a small number of minimal addition chains. *Discrete Mathematics*, 205(1–3), 221–227.

[7] Flammenkamp, A. (2020, June 7). *Shortest addition chains*. Universität Bielefeld personal webpage. `http://wwwhomes.uni-bielefeld.de/achim/addition-chain.html`

[8] Gioia, A., Subbarao, M., & Sugunamma, M. (1962). The Scholz–Brauer problem in addition chains. *Duke Mathematical Journal*, 29, 481–487.

[9] Knuth, D. E. (1997). *The Art of Computer Programming: Seminumerical Algorithms* (3 ed. Vol. 2, pp. 461–485). MA, Reading: Addison-Wesley.

[10] Scholz, A. (1937). Jahresbericht. *Jahresbericht der deutschen Mathematiker-Vereinigung*, 47(2), 41–42.

[11] Subbarao, M. (1989). Addition chains – some results and problems. In Mollin, R. A. (Ed.) *Number Theory and Applications* (pp. 555–574). Dordrecht: Kluwer Academic Publishers.

[12] Thurber, E. G. (1973). The Scholz–Brauer problem on addition chains. *Pacific Journal of Mathematics*, 49(1), 229–242.

[13] Utz, W. R. (1953). A note on the Scholz–Brauer problem on addition chains. *Proceedings of the American Mathematical Society*, 4, 462–463.