

On the Number of Minimal Addition Chains

Hatem M. Bahig

Computer Science Division, Department of Mathematics,
Faculty of Science, Ain Shams University, Cairo, Egypt.
hmbahig@asunet.shams.edu.eg

Abstract—An addition chain for a natural number n is a sequence $1 = a_0 < a_1 < \dots < a_r = n$ of numbers such that for each $0 < i \leq r$, $a_i = a_j + a_k$ for some $0 \leq k \leq j < i$. Thurber [9] introduced the function $NMC(n)$ which denotes the number of minimal addition chains for a number n . Thurber calculated $NMC(n)$ for some classes of n , such as when n has one or two ones in its binary representation. Also, he calculated $NMC(2^m n)$, for $n \in X = \{2, 3, 5, 9, 15, 17, 33, 49, 51, 65, 85, 97, 99\}$. For odd n does not belong to X and less than or equal to 127, he conjectured formula for $NMC(2^m n)$. In this paper, we verified the conjectures computationally up to $m = 150$ for each n . For $n = 69, 75$, and 109 the minimum value of m is corrected. For $n = 57$, and 111, the formula for NMC is corrected (there is a mistyping).

keywords: addition chain, number of minimal addition chains, Thurber's conjecture.

I. INTRODUCTION

An addition chain [5][7] for a natural number n is a sequence $1 = a_0 < a_1 < \dots < a_r = n$ of numbers such that for each $0 < i \leq r$, $a_i = a_j + a_k$ for some $0 \leq k \leq j < i$. The number of steps r is called the *length* of the addition chain for n . The minimal length for which there exists an addition chain for n is denoted by $\ell(n)$.

Let $\lambda(n) = \lfloor \log_2 n \rfloor$ and $\nu(n)$ be the number of 1's in the binary representation of n . The i^{th} step $a_i = a_j + a_k$ ($0 \leq k \leq j < i$) is called *doubling* if $j = k = i - 1$; *star* if $j = i - 1$; *small* if $\lambda(a_i) = \lambda(a_{i-1})$; and *big* if $\lambda(a_i) = \lambda(a_{i-1}) + 1$.

The length of an addition chain can be expressed as [5]:

$$r = \lambda(n) + S(a_0, a_1, \dots, a_r = n),$$

where $S(a_0, a_1, \dots, a_i)$ denotes the number of small steps in the chain up to a_i .

Clearly, this definition can be extended to (nonempty finite) set of numbers as follows:

Without loss of generality, we assume that $A = \{n_1, n_2, \dots, n_k\}$ be a set of k -numbers such that $2 \leq n_i < n_{i+1}$, for $1 \leq i < k$. An addition chain for a set A (in this case we call it an *addition sequence* for A) is an addition chain for the maximum element of A containing every element of A . We will denote the length of addition sequence of A by $\ell(A)$.

The problem of finding a minimal addition chain for a set of m -numbers $\{n_1, n_2, \dots, n_m\}$ is NP-complete [2]. This does not imply as it is sometimes claimed that finding a minimal addition chain for n is NP-complete. However, we can easily deduce that the problem of finding all minimal addition chains for a number n is NP-complete. Generating all minimal addition chains may help us to answer some open problems in addition chains, such as, *is there a natural number n such that $\ell(n) < \ell^o(n)$ where $\ell^o(n)$ is the minimum length of the so-called ℓ^o -chains?* Also, it may help us to find some sufficient conditions for star steps. Finding such conditions may speed up the generation of all (or one) minimal addition chains [1].

Thurber [9] introduced the function $NMC(n)$ which denotes the number of minimal addition chains for a number n . Thurber calculated a lower bound of $NMC(n)$ for normal numbers n for which the factor chain method [5] generates a minimal addition chain. For n with one or two ones in its binary representation, he calculated $NMC(n)$. Also, he calculated $NMC(2^m n)$, for $n \in X = \{2, 3, 5, 9, 15, 17, 33, 49, 51, 65, 85, 97, 99\}$. For odd n does not belong to X and less than or equal to 127, he conjectured NMC as shown in Table I. A. Flammenkamp [3] showed that the only numbers that have only one minimal addition chain are 2^k and 3. Also, he characterized n that have only two minimal chains.

In this paper, we verified Thurber's conjectures $NMC(2^m n)$ (Table I) up to $m = 150$ for each odd

$n \notin X$ and $n \leq 127$.

This paper is organized as follows. Section II, we briefly mention how to generate all minimal addition chains using [10][1]. Studying Thurber's conjecture computationally is presented in Section III. Section IV includes the conclusion.

II. GENERATING ALL MINIMUM ADDITION CHAINS

In this section, we describe how to generate all minimal addition chains and so how to calculate NMC. The algorithm traverses a search tree using depth-first search technique where some branches can be omitted by theoretical considerations called pruning bounds (or bounding sequence) [10, Table 3]. The algorithm uses a stack to hold the possible children a_{i+1} of a_i at each stage. The children of a_i constitute a stack segment. The stack holds initially the number $a_0 = 1$, since any addition chain starts with $a_0 = 1$. At each stage, the possible children a_{i+1} of a_i are put in the stack, where the possible values of a_{i+1} are all sums $a_{i+1} = a_j + a_k$ for $k \leq j \leq i$, such that:

- 1) $a_i < a_{i+1} \leq n$; and
- 2) $a_{i+1} \geq b_{i+1}$, and $a_{i+1} + a_i \geq b_{i+2}$, where $\{b_i\}_{i=1}^{lb}$ is the bounding sequence for n (see [10, Table 3]). The bounding sequence determines a lower bound of each a_i in addition chains of n with length lb . The bounding sequence depends on n and the lower bound lb of $\ell(n)$. If $a_{i+1} \leq b_{i+1}$, or $a_{i+1} + a_i \leq b_{i+2}$ (under some conditions in some bounding sequences [10, Table 3]), then the partial chain a_0, a_1, \dots, a_{i+1} cannot lead to a minimal chain for n .

The algorithm is as follows:

Algorithm: Generating all minimal addition chains

Input: n

Output: $\text{NMC}(n)$

Begin

if $\nu(n) \leq 16$ **then**

$lb \leftarrow \lambda(n) + \lceil \log_2 \nu(n) \rceil$ (see [8]);

else $lb \leftarrow \lceil \log_2 n + \log_2(\nu(n)) - 2.13 \rceil$ (see [6]);

end if

$a_0 \leftarrow 1$;

$a_1 \leftarrow 2$;

$\text{NMC} \leftarrow 0$;

loop

Determine the bounding sequence $B = \{b_i\}_{i=1}^{lb}$

$i \leftarrow 1$;

loop find-chain

if $(i < lb)$ **then**

Determine whether to retain a_i ;

if a_i is retained **then**

Put in the stack the possibilities for a_{i+1} ;

$i \leftarrow i + 1$;

$a_i \leftarrow$ the element on top of the stack;

if $a_i = n$ **then**

$\text{NMC} \leftarrow \text{NMC} + 1$;

take the next element off the stack that is not in the stack segment of a_i ;

end if

else

Take the next element off the stack;

$a_i \leftarrow$ the element on top of the stack;

end if

else

Take the next element off the stack that is not in the stack segment of a_i ;

$a_i \leftarrow$ the element on top of the stack;

end if

end loop find-chain

if no chains found **then** $lb \leftarrow lb + 1$;

else return NMC ;

end if

end loop

End.

To speedup generation of a_{i+1} , the bounding sequence should be used before pushing the possible children of a_i in the stack. Bahig [1] generated all a_{i+1} into two steps, one for stars and the other for nonstars. Then he

- 1) proposed to use (efficient) sufficient conditions for stars. If a sufficient condition for star is satisfied, then no need to generate nonstar steps.
- 2) defined and computed (what he called) the *non-star lower bound* of a_{i+1} using the lower bounds of k , and j , since $0 \leq k \leq j \leq i - 1$. Thus, in order to speed up generation of nonstar, we can restrict the generation to the lower bound.

III. THURBER'S CONJECTURE

For odd $n \leq 127$ and $n \notin X = \{2, 3, 5, 9, 15, 17, 33, 49, 51, 65, 85, 97, 99\}$, Thurber [9] conjectured formula for $\text{NMC}(2^m n)$ as shown in Table I. We implemented [10][1] using GMP [4] to verify the conjectures computationally up to $m = 150$ for each n . We found that the conjectures (as in Table I) are true up to $m = 150$, except in the following cases we need to modify them.

- 1) In case of $n = 57$, there is a mistyping. $\text{NMC}(2^m \times 57) = 73m^2 + 285m + \underline{150}$, for $m \geq 2$.
- 2) In case of $n = 69$, m should be greater than or equal to 3 (not 2). If $m = 2$ (as in [9]), then $\text{NMC} = 131$, but we have found that $\text{NMC} = 135$.
- 3) In case of $n = 75$, it is valid for $m \geq 0$ (not 3).

- 4) In case of $n = 109$, $m \geq 3$ (not 0). If $m = 0$, then we get a negative value for NMC which is a contradiction. If $m = 1$, or 2, then $NMC = 333$, 683 respectively, but we have found $NMC = 375$ and 687 respectively.
- 5) In case of $n = 111$, there is a mistyping. $NMC = 79m^2 + 135m + 96$. In fact, if $NMC = 79m^2 + 13m + 96$ and (for example) $m = 1$, or 2, then $NMC = 188$, 438 respectively, but we have found $NMC = 310$, 682 respectively.

IV. CONCLUSION

For odd $n \leq 127$, and $n \notin \{3, 5, 9, 15, 17, 33, 49, 51, 65, 85, 97, 99\}$, we have verified Thurber's conjectures ($NMC(2^m n)$) computationally up to $m = 150$. For $n = 69, 75$, and 109 the minimum value of m is corrected. For $n = 57$, and 111, the formula of NMC is corrected.

REFERENCES

- [1] H. Bahig, Improved generation of minimal addition chains. *submitted*.
- [2] P. Downey, B. Leong and R. Sethi, Computing sequences with addition chains, *SIAM J. Computing* Vol.10, No.3, pp. 638–646, 1981.
- [3] A. Flammenkamp, Integers with a small number of minimal addition chains. *Discrete Math.* 205, pp. 221–227, 1999.
- [4] GNU MP "The GNU Multiple Precision Arithmetic Library 4.1.4" <http://www.swox.com/gmp>
- [5] D. E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*. Vol.2, 3rd ed., Addison-Wesley, Reading MA, pp. 461–485, 1997.
- [6] A. Schönhage, A lower bound for the length of addition chains, *Theoretical Computer Science* **1**, pp. 1–12, 1975.
- [7] M. Subbarao, Addition chains—some results and problems. in *Number Theory and Applications*, R.A. Mollin, ed., Kluwer Academic Publishers, Dordrecht, pp. 555–574, 1989.
- [8] E.G. Thurber, The Scholz-Brauer problem on addition chains. *Pacific J. Math.* **49**, pp. 229–242, 1973.
- [9] E.G. Thurber, Addition chains—an erratic sequence. *Discrete Math.* **122**, pp. 287–305, 1993.
- [10] E.G. Thurber, Efficient generation of minimal length addition chains. *SIAM J. Computing* **28**, pp. 1247–1263, 1999.

TABLE I
THURBER'S CONJECTURES

n	$\text{NMC}(2^m n)$	valid for $m \geq$	correction
7	$9m + 5$	0	
11	$29m + 11$	1	
13	$14m + 10$	0	
19	$73m + 15$	2	
21	$9m^2 + 50m + 25$	1	
23	$4m + 4$	0	
25	$2m^2 + 20m + 14$	0	
27	$(m^3 + 18m^2 + 47m + 30)/6$	0	
29	$275m + 69$	2	
31	$190m + 39$	2	
35	$18m^2 + 93m + 7$	3	
37	$79m + 21$	2	
39	$14m^2 + 34m + 20$	0	
41	$35m + 19$	1	
43	$4m + 4$	0	
45	$m^3 + 10m^2 + 23m + 14$	0	
47	$534m + 81$	3	
53	$458m + 17$	3	
55	$58m^2 + 429m + 2$	3	
57	$73m^2 + 285m + 159$	2	$73m^2 + 285m + 150$
59	$63m + 33$	1	
61	$202m + 53$	2	
63	$(9m^3 + 140m^2 + 297m + 174)/2$	0	
67	$63m - 41$	4	
69	$4m^2 + 61m - 7$	2	$m \geq 3$
71	$4444m - 1734$	5	
73	$93m + 31$	2	
75	$2m^3 + 26m^2 + 56m + 32$	3	$m \geq 0$
77	$4m + 4$	0	
79	$1848m - 204$	4	
81	$(m^4 + 34m^3 + 227m^2 + 1346m + 768)/24$	1	
83	$4m + 4$	0	
87	$275m^2 + 1123m + 169$	4	
89	$971m + 158$	3	
91	$126m^2 + 1164m - 142$	4	
93	$190m^2 + 549m + 264$	2	
95	$146m^2 + 270m + 192$	1	
101	$732m - 203$	4	
103	$400m - 271$	4	
105	$18m^3 + 201m^2 + 548m + 292$	2	
107	$84m$	2	
109	$350m - 17$	0	$m \geq 3$
111	$79m^2 + 13m + 96$	1	$79m^2 + 135m + 96$
113	$212m + 104$	2	
115	$8m^2 + 71m + 37$	1	
117	$7m^3 + 64m^2 + 147m + 86$	0	
119	$18m^2 + 38m + 20$	0	
121	$247m + 78$	2	
123	$35m^2 + 95m + 64$	0	
125	$(4m^3 + 108m^2 + 248m + 144)/3$	0	
127	$11158m - 5131$	5	