MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 17–23

A CONJECTURE IN ADDITION CHAINS RELATED TO SCHOLZ'S CONJECTURE

WALTER AIELLO AND M. V. SUBBARAO

Dedicated to the memory of D. H. Lehmer

ABSTRACT. Let $l(n)$ denote, as usual, the length of a shortest addition chain for a given positive integer n. The most famous unsolved problem in addition chains is Scholz's 1937 conjecture that for all natural numbers n, $l(2^n - 1) \leq l(n) + n - 1$. While this conjecture has been proved for certain classes of values of n, its validity for all n is yet an open problem. In this paper, we put forth a new conjecture, namely, that for each integer $n \geq 1$ there exists an addition chain for $2^n - 1$ whose length equals $l(n) + n - 1$. Obviously, our conjecture implies (and is stronger than) Scholtz's conjecture. However, it is not as bold as conjecturing that $l(2^n - 1) = l(n) + n - 1$, which is known to hold, so far, for only the twenty-one values of n which were obtained by Knuth and Thurber after extensive computations. By utilizing a series of algorithms we establish our conjecture for all $n \leq 128$ by actually computing the desired addition chains. We also show that our conjecture holds for infinitely many n, for example, for all n which are powers of 2.

1. INTRODUCTION

A sequence of positive integers $1 = a_0 < a_1 < \cdots < a_r = n$ is said to be an addition chain for n if for each step i, $1 \leq i \leq r$, we have $a_i = a_j + a_k$ for some j, k such that $k \leq j < i$. The integer r is called the length of the addition chain for n. The minimal value of r for all possible addition chains for n is denoted by $l(n)$.

In 1937, Scholz [6] conjectured that, for all $n \geq 1$, we have

$$l(2^n - 1) \leq l(n) + n - 1. \tag{1.1}$$

Many of the investigations in addition chains concern this celebrated conjecture.

Now, let the binary representation of $n > 1$ be

$$n = 2^{c_0} + 2^{c_1} + \cdots + 2^{c_t}, \qquad c_0 > c_1 > \cdots > c_t \geq 0. \tag{1.2}$$

Following Knuth [4], we write

$$\lambda(n) = \left[\frac{\log n}{\log 2}\right] = [\log_2 n] = c_0 \tag{1.3}$$

Received by the editor July 27, 1992.
1991 *Mathematics Subject Classification.* Primary 11B83; Secondary 11Y55.
Key words and phrases. Addition chain, Scholz conjecture, short chain.
Research supported in part by an NSERC grant.

0025-5718/93 $1.00 + $.25 per page

and

(1.4) $\nu(n) = t + 1 =$ the number of ones in the binary representation of n.

(1.5) The ith step $a_i = a_j + a_k$ $(k \leq j < i)$ is called (i) a simple step if $j = i - 1$, $k = 1$ and (ii) a star step if $j = i - 1$, and (iii) a "doubling" if $j = k = i - 1$.

(1.6) A chain for n is a star chain provided all its steps are star steps.

(1.7) $l^*(n)$ denotes the length of a minimal star chain for n. (An integer n may have more than one star chain of minimal length.)

D. H. Lehmer [5] suggested the problem of finding the minimum of $\varepsilon s + (r - s)$, where $r =$ length of an addition chain for n, and $s =$ number of simple steps and ε is a parameter. Note that for $\varepsilon = 1$ this reduces to the study of $l(n)$.

The Scholz conjecture (1.7) is now known to be true for all integers n with $\nu(n) \leq 4$. The results for $\nu(n) = 1$ or 2 are due to Utz [9], for $\nu(n) = 3$ to Gioia, Subbarao and Sugunamma [2]; and for $\nu(n) = 4$ the results are due to Knuth [4]. In addition, the Scholz conjecture has been proved by A. Brauer [1] to hold for all n for which $l(n) = l^*(n)$. It may be noted that for all n for which $\nu(n) \leq 4$ we have $l(n) = l^*(n)$. Optimistic people hoped this equality would hold for all n.

However, Hansen [3] proved the astonishing result that $l(n) < l^*(n)$ for infinitely many n. Define a Hansen chain for an integer n as one in which certain elements in the chain are underlined and such that each member of the chain after the first uses the largest underlined element less than the member as a summand. Hansen proved that Scholz's conjecture is true for integers n that include a Hansen chain among their minimal chains. Such integers n are called Hansen numbers. A challenging open question now is whether or not there exist non-Hansen numbers.

Every known integer n for which $l(n) < l^*(n)$ is a Hansen number. Knuth found that the first five numbers n for which $l(n) < l^*(n)$ are 12509, 13207, 13705, 15473 and 16537. Thurber [8] found more such numbers including 20753, 23447, 24797, 26391, 27401, 30897, 31001, 32921, 33065 and 33074. But all these numbers being Hansen numbers satisfy the Scholz conjecture.

The solutions of the equation

$$l(2^n - 1) = l(n) + n - 1 \tag{1.8}$$

have also attracted some attention. Knuth used extensive computations to show that (1.8) holds for all $n \leq 14$. Thurber [8] extended this list by showing that $n = 15, 16, 17, 18, 20, 24, 32$ also satisfy (1.8). Stolarsky [7] conjectured that

$$l(n) \geq \lambda(n) + \log_2 \nu(n). \tag{1.9}$$

If this conjecture holds, one can show that equation (1.8) has infinitely many solutions n including those for which $\nu(n) = 1$ or 2.

2. Short chain for $(2^n - 1)$ and Conjecture C

A chain for $2^n - 1$ is said to be "short" if its length equals $l(n) + n - 1$, which we shall call Scholz's number and denote it by $S(n)$. We now propose:

2.1. **Conjecture** C. For every $n \geq 1$, the number $2^n - 1$ has a short chain.

2.2. *Remark.* Obviously, Conjecture C implies and is stronger than Scholz's conjecture. If a short chain for $2^n - 1$ is also the shortest chain for $2^n - 1$, then of course it provides a solution for (1.8).

We now state a series of algorithms which help us to actually construct short chains for $2^n - 1$.

Utilizing these, we prove conjecture C for all $n \leq 128$ and also for n which are powers of 2.

2.3. **Definition.** A reverse addition chain for $2^n - 1$ is a decreasing sequence of numbers beginning with $2^n - 1$ and ending with unity which, when the order is reversed, becomes an addition chain for $2^n - 1$.

2.4. **Definition.** A *segment* of a reverse addition chain for $2^n - 1$ is a sequence $\{D_1, D_2, \ldots, D_s\}$ of integers $D_1 > D_2 > \cdots > D_s \geq 1$ such that each D-term can be expressed as the sum of two succeeding D's, or the sum of a succeeding D-term and unity. Note that unity need not be the last term of a segment. Formally, this means that for $1 \leq i \leq s - 1$, $D_i = D_j + D_k$, $i < j \leq k \leq s$, or $D_i = D_j + 1$, $i < j \leq s$. The "length" of the segment is s—the number of terms in it.

Remark. Our method of constructing a reverse addition chain for $2^n - 1$ mainly consists of constructing successive suitable segments and putting them together; each segment begins and ends with numbers of the form $2^b - 1$. This procedure, however, may not work for some n, and then, we have to use other devices.

2.5. **Algorithm I.** This is for constructing a segment for $2^n - 1$, n odd. Set $m = (n + 1)/2$ and

$$C_1 = 2^n - 1,$$
$$C_2 = (2^n - 1) - (2^m - 1) = 2^m + \cdots + 2^{n-1}.$$

The next $m - 2$ terms are constructed by successive "halfings," so that $C_3 = \frac{1}{2}C_2, \ldots, C_m = 2^2 + \cdots + 2^{(n+1)/2}$. Next set

$$C_{m+1} = 2^m - 1,$$
$$C_{m+2} = \tfrac{1}{2}C_m = (2^m - 1) - 1,$$
$$C_{m+3} = \tfrac{1}{2}C_{m+2} = 2^{m-1} - 1.$$

Note that

$$C_1 = C_2 + C_{m+1},$$
$$C_{m+1} = C_{m+2} + 1,$$
$$C_{m+2} = 2C_{m+3}.$$

Thus, $\{C_1, C_2, \ldots, C_{m+3}\}$ is a valid step-down segment. To construct the next segment, we begin with $2^{m-1} - 1$.

2.6. **An alternative to Algorithm I.** We set

$$C_1 = 2^n - 1 \quad (n \text{ odd}).$$

Set $r = (n-1)/2$ and

$$C_2 = (2^n - 1) - (2^r - 1) = 2^r + \cdots + 2^{n-1},$$
$$C_3 = \tfrac{1}{2}C_2 = 2^{r-1} + \cdots + 2^{n-2},$$
$$C_4 = \tfrac{1}{2}C_3,$$
$$C_5 = \tfrac{1}{2}C_4,$$
$$\cdots\cdots$$
$$C_{r+2} = 2^0 + \cdots + 2^{n-r-1} = 2^{n-r} - 1 = 2^{(n+1)/2} - 1.$$

We next define

$$C_{r+3} = C_{r+2} - 1 = 2^{(n+1)/2} - 2,$$
$$C_{r+4} = \tfrac{1}{2}C_{r+3} = 2^r - 1.$$

The length of the segment $\{C_1, \ldots, C_{r+4}\}$ is $= r + 3 = \frac{n+5}{2} =$ the same length as for the segment in 2.5. Analogous to star chains, we may say that the segment $\{C_1, \ldots, C_{r+4}\}$ is a "star" segment.

2.7. **Algorithm** II. This method is used if n is even. Let $m = n/2$ and set

$$C_1 = 2^n - 1,$$
$$C_2 = (2^n - 1) - (2^m - 1) = 2^m + \cdots + 2^{n-1}.$$

Divide by 2 successively m times to get $C_3 = \frac{1}{2}C_2, \ldots,$

$$C_{m+2} = 2^0 + \cdots + 2^{n/2-1} = 2^m - 1.$$

We now have a valid segment $\{C_1, C_2, \ldots, C_{m+2}\}$, where $C_1 = C_2 + C_{m+2}$. We can then apply a suitable algorithm to $2^m - 1$. Note that the number of elements in this segment is $m + 2$.

Before proceeding to the other algorithms we prove

2.8. **Theorem.** *Conjecture C holds for all integers n which are powers of* 2.

Proof. Let $n = 2^a$, a being a positive integer. Applying Algorithm II successively $a - 2$ times and adding up the lengths of all the segments, with due care to avoid duplication in counting the elements, we get this sum as

$$(2^{a-1} + 1) + (2^{a-2} + 1) + \cdots + (2^1 + 1) + (2^0 + 1) = 2^a - 1 + a = n - 1 + l(n),$$

since $l(2^a) = a$; the theorem follows at once. □

2.9. **Algorithm** III. This is to be tried when $3|n$, and $n > 6$. Usually, this gives a shorter segment than Algorithm I. Set $m = \frac{2n}{3}$ and

$$C_1 = 2^n - 1,$$
$$C_2 = (2^n - 1) - (2^m - 1) = 2^m + \cdots + 2^{n-1}.$$

Dividing by 2 a total of $(\frac{n}{3} - 1)$ times, we get

$$C_{n/3+1} = 2^{n/3+1} + \cdots + 2^{2n/3}.$$

Then set $C_{n/3+2} = 2^{m-1} = 2^0 + \cdots + 2^{2n/3-1}$. Then for elements $C_{n/3+3}, \ldots,$ C_{m+3} we successively divide $C_{n/3+1}$ by two $\frac{n}{3} + 1$ more times so that $C_{n/3+3} =$

$2^{n/3} + \cdots + 2^{2n/3-1}$, and finally, $C_{2n/3+3} = C_{m+3} = 2^0 + \cdots + 2^{n/3-1} = 2^{n/3} - 1$. We then have a valid segment going from $2^{n/3} - 1$ to $2^n - 1$, since

$$C_1 = C_2 + C_{n/3+2},$$
$$C_{n/3+2} = C_{m+3} + C_{n/3+3},$$

and the rest of the elements in the segment are obtained by doubling some other element.

2.10. **Algorithm** IV. This is to be tried when n is odd and sufficiently large. However, use of this method does not always give us a valid segment, since a 7 is needed at one point to step from one element to another. Thus a 7 must be present in the final chain in order for the construction to be valid.

Here we set $m = \frac{n+3}{2}$ and

$$C_1 = 2^n - 1 = 2^0 + \cdots + 2^{n-1},$$
$$C_2 = (2^n - 1) - (2^m - 1) = 2^m + \cdots + 2^{n-1}.$$

Divide by 2 successively $m - 4$ $(= \frac{n-5}{2})$ times to get

$$C_{m-2} = 2^4 + \cdots + 2^{(n+3)/2}.$$

Then set $C_{m-1} = 2^{(m+3)/2} - 1 = 2^0 + \cdots + 2^{(n+3)/2-1}$, and divide C_{m-2} by 2 four more times to get

$$C_m = 2^3 + \cdots + 2^{(n+3)/2-1}$$

and

$$C_{m+3} = 2^0 + \cdots + 2^{(n-3)/2-4} = 2^{(n-3)/2} - 1 = 2^m - 1.$$

So $C_1 = C_2 + C_{m-1}$, but in order to get $C_{m-1} = 2^0 + \cdots + 2^{(n+3)/2-1}$, we must add $7 = 2^0 + 2^1 + 2^2$ to $C_m = 2^3 + \cdots + 2^{(n+3)/2-1}$. Thus we do not have a valid segment unless one of the C_i's equals 7, and if we include this string in our construction we must ensure that a 7 appears in the final result to have a valid addition chain.

2.11. **Algorithm** V. This algorithm is similar to Algorithm IV and is used when n is odd and sufficiently large. As in Algorithm IV, use of this method does not always give a valid segment, the presence of a 31 being needed. Thus we must ensure that a 31 appears in the final result for that result to be a valid addition chain if use of this method is part of the process of construction.

Take $m = \frac{n+5}{2}$. Then set

$$C_1 = 2^{n-1},$$
$$C_2 = (2^n - 1) - (2^m - 1) = 2^m + \cdots + 2^{n-1}.$$

Divide by 2 a total of $(m - 6)$ times to get

$$C_{m-4} = 2^6 + \cdots + 2^{(n+5)/2}.$$

Then set $C_{m-3} = 2^0 + \cdots + 2^{(n+5)/2-1} = 2^{(n+5)/2} - 1$.

Divide C_{m-4} by 2 six more times to get $C_{m-2} = 2^5 + \cdots + 2^{(n+5)/2-1}$ and finally

$$C_{m+3} = 2^0 + \cdots + 2^{(n-3)/2-1} = 2^{(n-3)/2} - 1.$$

Now, $C_1 = C_2 + C_{m-3}$, $C_{m-3} = C_{m-2} + 31$, and all other elements in the chain are obtained by doubling some existing element.

We can now apply a suitable algorithm to $C_{m+3} = 2^{(n-3)/2} - 1$ to continue the process, if needed.

2.12. **Algorithm VI.** Again, this method is similar to Algorithms IV and V except that this time we take $m = \frac{n+7}{2}$. Now we must ensure that 127 be present in the final result in order to have a valid addition chain.

Take $m = \frac{n+7}{2}$ and set

$$C_1 = 2^n - 1 \quad \text{and} \quad C_2 = 2^m + \cdots + 2^{n-1}.$$

Successively divide by 2 a total of $m-8$ times to get $C_{m-6} = 2^8 + \cdots + 2^{(n+7)/2}$. Then set $C_{m-5} = 2^0 + \cdots + 2^{(n+7)/2-1}$ and successively divide C_{m-6} by 2 eight more times to get

$$C_{m-5} = 2^7 + \cdots + 2^{(n+7)/2-1}$$

and

$$C_{m+3} = 2^0 + \cdots + 2^{(n-7)/2-1} = 2^{(n-7)/2} - 1.$$

Here $C_1 = C_2 + C_{m-5}$ and $C_{m-5} = C_{m-4} + 127$. We can apply an appropriate algorithm to C_{m+3} if necessary. The final result will be a valid addition chain only if a 127 appears in that result.

2.13. **Special methods.** For $n = 33, 77$, and 129 no combination of Algorithms I–VI yields a short chain. Special methods must then be employed. If a segment or string terminates at $2^m - 1 = 33$ or 77, we apply one of these methods to obtain a final, short chain.

For $n = 33$ and 77 we exhibit valid short chains in the Supplement section at the end of the Appendix.

A complete list of short chains for all $n \leq 128$ is available from the authors. The algorithms used for the generation of these short chains for $n \leq 128$ are shown in the Appendix.

2.1.4. We would like to note that these methods, although demonstrated for n only up to 128, will produce valid short chains for some n higher than 128. Indeed, we conjecture that the use of these methods, coupled with other similar algorithms, would suffice to give short chains for arbitrarily large n.

ACKNOWLEDGMENT

We would like to acknowledge our indebtedness to D. E. Knuth whose multiple-precision algorithms formed part of a library of multiple-precision integer routines on our computer system. This library was used by the programs that computed the short addition chains which we exhibit here.

BIBLIOGRAPHY

1. A. T. Brauer, *On addition chains*, Bull. Amer. Math. Soc. **45** (1939), 736–739.
2. A. A. Gioia, M. V. Subbarao, and M. Sugunamma, *The Scholz-Brauer problem in addition chains*, Duke Math. J. **29** (1962), 481–487. See also A. A. Gioia and M. V. Subbarao, *The Scholz-Brauer problem in addition chains*. II, Proc. Eighth Manitoba Conf. on Numerical Math. and Computing, 1978, pp. 174–251.
3. W. Hansen, *Zum Scholz-Brauerschen problem*, J. Reine Angew. Math. **202** (1959), 129–136.

4. D. E. Knuth, *The art of computer programming*, 2nd ed., Addison-Wesley, Reading, Mass., 1969, pp. 398–422. (Second printing has some updates.)
5. D. H. Lehmer, See problem number 13 on page 421 of Knuth, where this problem is outlined.
6. A. Scholz, *Jahresbericht*, Deutsche Mathematiker Vereinigung, Aufgabe 252, **47** (1937), 41–42.
7. K. B. Stolarsky, *A lower bound for the Scholz-Brauer problem*, Canad. J. Math. **21** (1969), 675–683.
8. E. G. Thurber, *Additional chains and solutions of* $l(2n) = l(n)$ *and* $l(2^n - 1) = n + l(n) - 1$, Discrete Math. **16** (1976), 279–289.
9. W. R. Utz, *A note on the Scholz-Brauer problem in addition chains*, Proc. Amer. Math. Soc. **4** (1953), 462–463.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ALBERTA, EDMONTON, ALBERTA, CANADA T6G 2G1
E-mail address, W. Aiello: userwalt@mts.ucs.ualberta.ca
E-mail address, M. V. Subbarao: usersubb@mts.ucs.ualberta.ca