Discrete Mathematics 16 (1976) 279–289.

ADDITION CHAINS AND SOLUTIONS OF $l(2n)=l(n)$ AND $l(2^n-1)=n+l(n)-1$

Edward G. THURBER
Biola College, 13800 Biola Avenue, La Mirada, Calif. 90639, U.S.A.

Received 13 January 1975
Revised 9 January 1976

An addition chain for a positive integer n is a set $1=a_0<a_1<\ldots<a_r=n$ of integers such that for each $i\geq 1$, $a_i=a_j+a_k$ for some $k\leq j<i$. The smallest length r for which an addition chain for n exists is denoted by $l(n)$. This paper introduces the function $h(x)$ which denotes the number of integers n less than or equal to x for which $l(2n)=l(n)$ and proves that $h(x)\gg(\log_2 x)^2$. A necessary theorem for establishing this result is that there exist infinitely many infinite classes of integers for which $l(2n)=l(n)$. The proof of this theorem is outlined. Also, this paper establishes seven new cases for which $l(2^n-1)=n+l(n)-1$. These are cases $n=15$, 16, 17, 18, 20, 24 and 32.

1. Introduction

The study of how to raise x up to x^n most efficiently gives rise to the concept of the addition chain which for a positive integer n is a set $1=a_0<a_1<\ldots<a_r=n$ of integers such that for each $i\geq 1$, $a_i=a_j+a_k$ for some $k\leq j<i$. As x is raised up to x^n the exponents on the various powers of x form an addition chain. The minimal length r for which an addition chain for n exists is denoted by $l(n)$. This paper will investigate the equalities $l(2n)=l(n)$ and $l(2^n-1)=n+l(n)-1$ which are found to hold for certain values of n.

It was considered a remarkable fact when computer calculations revealed that $l(382)=l(191)=11$. It seems efficient to construct an addition chain for $2n$ by first constructing an addition chain for n and then adding n to itself to obtain $2n$. In fact, Utz [17] asks if it is not true that $l(n)<l(2n)$ for all $n\geq 1$. The computer calculations of Knuth reveal 39 integers ranging from 191 to 8971 for which $l(2n)=l(n)$. In [15] it is proved that there is an infinite class of integers for which $l(2n)=l(n)$. Specifically, if $n=2^m(23)+7$ where $m\geq 5$, then $l(2n)=l(n)=m+8$. If $h(x)$ denotes the number of integers n less than or equal to x for which $l(2n)=l(n)$, then this result implies that $h(x)\geq\log_2 x-10$ from which it follows that $h(x)\gg\log_2 x$. This paper will extend these results and show that there are infinitely many infinite classes of integers n for which $l(2n)=l(n)$ from which it will follow that $h(x)\gg(\log_2 x)^2$.

Let $\lambda(n)=[\log_2 x]$, and let $\nu(n)$ denote the number of ones in the binary representation of n. For each $i \geq 1$, it is clear that $a_i \leq 2a_{i-1}$. If $\lambda(a_i) = \lambda(a_{i-1})$, step i is called a small step while if $\lambda(a_i) = \lambda(a_{i-1}) + 1$ then step i is called a big step. These are the only possible relations between $\lambda(a_i)$ and $\lambda(a_{i-1})$, and as Knuth [9] points out the length r of an addition chain for n is $\lambda(n)$ plus the number of small steps in the chain. If $N(a_i)$ denotes the number of small steps in the chain up to a_i, then $r = \lambda(n) + N(n)$.

2. Proposition A

Four lemmas from [15] and Knuth's Theorem C in [9] will be referred to on a number of occasions. They are listed here for convenience. The first two lemmas concern integers written in their binary representation.

Lemma 1. *If $a_i = a_j + a_k$ and if c represents the number of carries in $a_j + a_k$, then $\nu(a_i) = \nu(a_j) + \nu(a_k) - c$.*

Before the next lemma is listed it needs to be mentioned that if a_j and a_k are written in binary notation and a_j is placed above a_k in order to add or subtract, the resultant figure is called a configuration and is designated by a_j/a_k. If for a given power of two a 1 appears in a_j over a 0 in a_k, this is called a 1/0 slot. If a 1 appears over a 1, this is called a 1/1 slot etc.

Lemma 2. *If $a_t = a_j - a_k$ and there are s 1/1 slots in a_j/a_k and a one appears in a_t exactly p times under either a 1/1 slot or a 0/0 slot, then $\nu(a_t) = \nu(a_j) - s + p$.*

Lemma 3. *If a_j and a_k are two members of an addition chain and if $\lambda(a_j) = \lambda(a_k) + m$ $(m \geq 0)$ and $2^m a_k < a_j$, then $N(a_j) \geq N(a_k) + 1$.*

Lemma 4. *If a_j and a_k are two members of an addition chain and if $\lambda(a_j) = \lambda(a_k) + m$ $(m \geq 2)$ and $a_j > 2^{m-1}a_k + 2^{m-2}a_k$, then $N(a_j) \geq N(a_k) + 1$ unless $a_j = 2^{m-1}a_{k+1}$.*

Theorem C. *If $\nu(n) \geq 4$, then $l(n) \geq \lambda(n) + 3$ except when $\nu(n) = 4$ and n has one of the four following binary forms:*

(A) *n = 1--d--1--1--d--1-- where d indicates the number of zeros between the first and second one and between the third and fourth one.*

(B) *n = 1--d--1--1--e--1-- where d and e again indicate zeros and $e = d - 1$.*

(C) *n = 1001--11-- where the dashes indicate zeros.*

(D) *n = 10000111-- where the dashes indicate zeros.*

In these four cases $l(n) = \lambda(n) + 2$.

It must be shown that there are infinitely many infinite classes of integers for which $l(2n) = l(n)$. This requires a tedious proposition whose proof will be outlined rather than done step by step. A more meticulous treatment of the methods involved can be found in [15].

Proposition A. *If $\nu(n) = 7$ and n has the binary representation n = 101--m--11--k--11--m--1 where m and k indicate the number of zeros between ones and $m \geq 1$ and $k \geq 3$, then $l(n) \geq \lambda(n) + 4$.*

In other words in any addition chain for an integer with these binary characteristics there will be at least four small steps.

Proof (Outline). Let $1 = a_0 < a_1 < \ldots < a_r = n$ be an addition chain for n where $\nu(n) = 7$ and n = 101--m--11--k--11--m--1 ($m \geq 1$, $k \geq 3$). By [15, Theorem 1] it can be assumed that all members of the chain have eight or less ones in their binary representation. If this were not the case and a certain member of the chain had more than eight ones in its binary representation, then by Theorem 1 there would be four small steps in the chain to this point and, hence, at least four small steps on the way to n. Let a_i denote the first member of the chain for which $\nu(a_i) = 7$ and a_i = 101--m--11--k--11--m--1 ($m \geq 1$, $k \geq 3$). It is quite possible that a_i is different from n since the values of m and k could be different from those for n. Now $a_i = a_j + a_k$ for some $k \leq j < i$. In fact, $k < j$ since a_i is odd and cannot be $2a_j$. Thus, a_j and a_k are distinct members of the chain, and $1 \leq \nu(a_j)$, $\nu(a_k) \leq 8$. It can easily be determined with the help of Lemma 1 that there are 49 possibilities for $(\nu(a_j), \nu(a_k))$ In each case it can be shown that $N(a_i) \geq 4$ from which it follows that $l(n) \geq \lambda(n) + 4$.

Certain cases such as (5, 2) are easy to dispense with. In this case there will be no carries in $a_j + a_k$ where a_j and a_k are in their binary representation. Thus, $\lambda(a_i) = \lambda(a_j)$ which means that there is a small step between a_j and a_i. In other words $N(a_i) \geq N(a_j) + 1$. By Theorem C, $N(a_j) \geq 3$ which implies $N(a_i) \geq 4$.

Case (6, 5) is a little more complex but not difficult. If there is to be a chance that $N(a_i) = 3$, then it must follow that $\lambda(a_i) = \lambda(a_j) + 1$ and $\lambda(a_j) > \lambda(a_k)$. If $\lambda(a_j) = \lambda(a_k)$, for instance, then there would be a small step between a_k and a_j, and by Theorem C this would imply $N(a_i) \geq 4$. By Lemma 3 it can be assumed that if $\lambda(a_j) = \lambda(a_k) + m$ for some $m \geq 1$ then $2^m a_k \geq a_j$. Otherwise $N(a_j) \geq N(a_k) + 1 \geq 4$. Also, by Lemma 1 there are four carries in the binary addition of $a_j + a_k$. With these restrictions placed on a_j and a_k there are two ways of obtaining a_i in the right form. These are:

$$
\begin{array}{rrl@{\qquad}rrl}
(1) & a_j = & \overleftarrow{1}\overleftarrow{1}\overleftarrow{1}00000\text{--} & (2) & a_j = & \overleftarrow{1}\overleftarrow{1}\overleftarrow{0}\overleftarrow{1}\text{--} \\
& + a_k = & 1111000\text{--} & & + a_k = & 111\text{--} \\
& a_i = & 101011000\text{--} & & a_i = & 10100\text{--}.
\end{array}
$$

The arrows above the configurations indicate carries. If $a_j = a_m + a_s$ for some $s \leq m < j$ where $a_m \neq a_k$ and if $a_k < a_m < a_j$, then it can be seen that there will be at least one small step between a_k and a_j. By Theorem C, $N(a_k) \geq 3$ which implies

$N(a_i) \geq 4$. If $a_m < a_k$, then $\lambda(a_m) = \lambda(a_k)$ since $2a_m \geq a_j$. This implies $N(a_k) \geq N(a_m) + 1$. Also, $N(a_m) \geq 3$ since if $N(a_m) \leq 2$ then $1 = a_0 < a_1 < \ldots < a_m < a_j$ would be an addition chain for a_j with less than three small steps, contradicting the fact that $N(a_j) \geq 3$ by Theorem C. Thus, $N(a_k) \geq 4$. If there is to be a chance that $N(a_i) = 3$, it must follow that $a_j = a_k + a_t$ for some $t \leq k < j$. Since the number of carries $c = 4$ in $a_t + a_k$, there is one more 1/1 slot in configuration (1) and no more in configuration (2). In either case, when a_k is subtracted from a_j to obtain a_t, it follows by Lemma 2 that $\nu(a_t) \geq 5$. Also, $\lambda(a_t) = \lambda(a_k)$, and $a_t \neq a_k$. Therefore, $N(a_k) \geq N(a_t) + 1 \geq 4$. In any event $N(n) \geq N(a_i) \geq 4$.

Certain of the other cases for $(\nu(a_j), \nu(a_k))$ are easier than (6, 5) to analyze and others are a bit more tedious. The more tedious cases are this way essentially since they involve more possibilities when they are broken down. They are analyzed, however, in the same manner. In light of the relation it has to what comes later, part of case (4, 3) will be discussed.

One of the ways of obtaining a_i in the right form in (4, 3) is with the following configuration:

$$\begin{aligned} a_j &= 101\text{--}m\text{--}11\text{--}k\text{--}00\text{--}m\text{--}0 \\ +\, a_k &= \phantom{101\text{--}m\text{--}11\text{--}k\text{--}}11\text{--}m\text{--}1 \\ a_i &= 101\text{--}m\text{--}11\text{--}k\text{--}11\text{--}m\text{--}1 \qquad (m \geq 1, k \geq 3). \end{aligned}$$

It can be seen that $\lambda(a_j) = \lambda(a_k) + m + k + 5$ while $a_j > 2^{m+k+4}a_k + 2^{m+k+3}a_k$. By Lemma 4, $N(a_j) \geq N(a_k) + 1$ unless $a_j = 2^{m+k+4}a_{k+1}$. This implies that 2^{m+k+4} divides a_j, but 2^{m+k+3} is the highest power of two that divides a_j. Thus, $N(a_j) \geq N(a_k) + 1$. It is easy to show that if $\nu(a_k) \geq 3$ then $N(a_k) \geq 2$ (see [9]). It follows that $N(a_i) \geq N(a_j) + 1 \geq 4$.

3. The equation $l(2n) = l(n)$

Proposition A gives a lower bound for $l(n)$ by showing that $l(n) \geq \lambda(n) + 4$. The following considerations will show that $\lambda(n) + 4$ is also an upper bound for $l(n)$.

If $\nu(n) = 7$ and $n = 101\text{--}m\text{--}11\text{--}k\text{--}11\text{--}m\text{--}1$ $(m \geq 1,\ k \geq 3)$, then n can be represented in powers of two as:

$$n = 2^{2m+k+7} + 2^{2m+k+5} + 2^{m+k+4} + 2^{m+k+3} + 2^{m+2} + 2^{m+1} + 1.$$

The following is an addition chain for n with four small steps:

$$\begin{aligned} &1, 2, 2^2, \ldots, 2^{m+2}, 2^{m+2} + 2^{m+1}, 2^{m+2} + 2^{m+1} + 1, 2^{m+3} + 2^{m+1} + 1, 2^{m+4} + 2^{m+2} + 2, \\ &2^{m+4} + 2^{m+2} + 2 + 1, 2(2^{m+4} + 2^{m+2} + 2 + 1), \ldots, 2^{m+k+3}(2^{m+4} + 2^{m+2} + 2 + 1), \\ &2^{m+k+3}(2^{m+4} + 2^{m+2} + 2 + 1) + 2^{m+2} + 2^{m+1} + 1 = n. \end{aligned}$$

This result combined with Proposition A proves that if $\nu(n) = 7$ and $n = 101\text{--}m\text{--}11\text{--}k\text{--}11\text{--}m\text{--}1$ $(m \geq 1,\ k \geq 3)$, then $l(n) = \lambda(n) + 4$.

It can be seen that $2n$ will have the same binary representation as n except that there will be an additional zero at the right end of the binary form of $2n$. In other words $\nu(2n) = 7$ and $2n = 101\text{--}m\text{--}11\text{--}k\text{--}11\text{--}m\text{--}10$ where $m \geqslant 1$ and $k \geqslant 3$. By Theorem C, $l(2n) \geqslant \lambda(2n) + 3$. On the other hand

$$\begin{aligned}&1, 2, 2^2, \ldots, 2^{m+2}, 2^{m+2}+1, 2^{m+3}+1, 2^{m+3}+2^{m+2}+2, 2^{m+4}+2^{m+2}+2+1,\\ &\quad 2(2^{m+4}+2^{m+2}+2+1), \ldots, 2^{m+k+4}(2^{m+4}+2^{m+2}+2+1),\\ &\quad 2^{m+k+4}(2^{m+4}+2^{m+2}+2+1)+2^{m+3}+2^{m+2}+2 = 2n\end{aligned}$$

is an addition chain for $2n$ with three small steps. Thus, $l(2n) = \lambda(2n) + 3$. Consequently,

$$l(2n) = \lambda(2n) + 3 = (\lambda(n) + 1) + 3 = \lambda(n) + 4 = l(n).$$

Since for each $m \geqslant 1$ there are an infinite number of $k \geqslant 3$, this establishes that there are infinitely many infinite classes of integers for which $l(2n) = l(n)$. This will be stated formally as a theorem.

Theorem 1. *For each $m \geqslant 1$, the set of integers with $\nu(n) = 7$ and n of the binary form $n = 101\text{--}m\text{--}11\text{--}k\text{--}11\text{--}m\text{--}1$ (where $k \geqslant 3$) is an infinite class of integers for which $l(2n) = l(n)$.*

The first integer for which Theorem 1 applies is 5517 which has the binary representation 1010110001101. $\lambda(5517) = 12$, and 5517 is the only integer in the half-open interval $[2^{12}, 2^{13})$ to which the theorem applies. There is one integer n for which $\lambda(n) = 13$ to which Theorem 1 applies. There are two integers each for which $\lambda(n) = 14$ and $\lambda(n) = 15$ to which Theorem 1 applies, and in general there are $m - 5$ integers each for $\lambda(n) = 2m$ and $\lambda(n) = 2m + 1$ to which Theorem 1 applies. The letter x will now replace n. If $\lambda(x) = 2m$ $(m \geqslant 6)$, Theorem 1 gives $2(1 + 2 + 3 + \ldots + (m-6)) + (m-5) = (m-5)^2$ integers in the interval $[1, 2^{2m+1})$ for which $l(2n) = l(n)$. If $\lambda(x) = 2m + 1$ $(m \geqslant 6)$, then Theorem 1 gives $2(1 + 2 + 3 + \ldots + (m-5)) = (m-5)(m-4)$ integers in the interval $[1, 2^{2m+2})$ for which $l(2n) = l(n)$. In either event it can be easily shown that there are at least $(\frac{1}{2}(\lambda(x) - 11))(\frac{1}{2}(\lambda(x) - 9))$ integers $(\lambda(x) \geqslant 12)$ in the interval $[1, 2^{\lambda(x)+1})$ for which $l(2n) = l(n)$. Thus, $h(2^{\lambda(x)+1}) \geqslant (\frac{1}{2}(\lambda(x) - 11))(\frac{1}{2}(\lambda(x) - 9))$.

The following lower bound for $h(2x)$ can now be developed.

$$h(2x) = h(2^{\log_2 x + 1}) \geqslant h(2^{\lambda(x)+1}) \geqslant (\tfrac{1}{2}(\lambda(x) - 11))(\tfrac{1}{2}(\lambda(x) - 9)).$$

If x is replaced by $\frac{1}{2}x$, the following inequality ensues:

$$h(x) \geqslant (\tfrac{1}{2}(\lambda(x) - 12))(\tfrac{1}{2}(\lambda(x) - 10)).$$

This inequality will still hold if $\lambda(x)$ is replaced by $\log_2 x - 1$, since $\lambda(x) > \log_2 x - 1$. If this is done, it follows that $h(x) \gg (\log_2 x)^2$.

It is highly probable that this result can be improved. It is conceivable that $h(x) \gg (\log_2 x)^n$ for arbitrarily large n. It might also be asked if

$$\liminf_{x\to\infty} h(x)/x > 0.$$

This seems to be a difficult question. The density in the positive integers of all positive integers with exactly seven ones in their binary representation is

$$\lim_{m\to\infty} \binom{m}{7} \Big/ 2^m = 0.$$

In particular the integers of Theorem 1 have zero density in the set of positive integers. An area where it seems that improvements can be made without too much difficulty is in lower bounds for $h(x)$. From Knuth's computer calculations, Theorem 1 of this paper and [15, Theorem 2], it follows that $h(100\,000) \geqslant 51$ and $h(1\,000\,000) \geqslant 65$. More theoretical work and improved computer programs should raise these bounds considerably.

An investigation into these questions might begin by looking at the nature of the binary representation of the integers for which $l(2n) = l(n)$. A method for forming minimal or near minimal addition chains for an integer n was discussed briefly in [16]. An integer n is written in its binary representation, and certain parts of it are underlined. The underlined parts are called critical numbers c_1, c_2, c_3 etc. The method consists of finding a minimal chain for c_1 which includes c_2, c_3 etc. and then doubling c_1 the appropriate number of times and adding in c_2, then doubling this result the appropriate number of times and adding in c_3 etc. until n is reached. As mentioned earlier, doubling an integer in its binary representation merely shifts all digits one place to the left and adds in a zero at the right end of the number. In Proposition A, n has the binary form $n = \underline{101\text{--}m\text{--}11}\text{--}k\text{--}\underline{11\text{--}m\text{--}1}$. As underlined, $c_1 = 101\text{--}m\text{--}11$ and $c_2 = 11\text{--}m\text{--}1$. The same technique that was used in the case considered in (4, 3) of Proposition A can be used here to show that a minimal chain for c_1 which contains c_2 has three small steps. The chain to n is finished by doubling c_1 a total of $m + k + 3$ times and then adding in c_2 which gives the fourth small step. If one considers $2n$ the underlining is as follows: $2n = \underline{101\text{--}m\text{--}11}\text{--}k\text{--}\underline{11\text{--}m\text{--}10}$. As has been shown, a minimal chain to $c_1 = 101\text{--}m\text{--}11$ which contains $2c_2 = 11\text{--}m\text{--}10$ has only two small steps. Thus, the chain for $2n$, though it will have one more doubling, will have one less small step; hence, as has been proved for integers with this binary form, $l(2n) = l(n)$. A search for more integers for which $l(2n) = l(n)$ might well begin by trying to find pairs (c_1, c_2) of integers for which a minimal chain to c_1 including c_2 requires one more step than one including $2c_2$. Some such pairs are (23, 7), (37, 7), (69, 7), (35, 11), (69, 21) and (67, 21). The pair (23, 7) leads to an infinite class of integers for which $l(2n) = l(n)$ as was proved in [15, Theorem 2]. It is highly probable that each of the other pairs also leads to an infinite class of integers for which $l(2n) = l(n)$.

4. The Scholz–Brauer conjecture

Perhaps the most famous of the unsolved problems concerning addition chains is the Scholz–Brauer conjecture which states that $l(2^n-1) \leq n + l(n) - 1$. Knuth's computer calculations have established that $l(2^n-1) = n + l(n) - 1$ for $n = 1$ to 14. It will now be shown that equality holds for the additional values $n = 15, 16, 17, 18, 20, 24$ and 32. Of these cases $n = 15$ is the most difficult to establish and will be saved for last.

In each case $2^n - 1 = a_j + a_k$ for some $k < j$. It is not possible that $k = j$ since $2^n - 1$ is odd and therefore is not equal to $2a_j$. This last step in an addition chain to $2^n - 1$ must be a small step since $2^n - 1$ consists of all ones in its binary representation and, hence, there can be no carries in $a_j + a_k$ where a_j and a_k are represented in their binary forms. If there were any carries, there would have to be at least one zero in the sum. Since there are no carries in $a_j + a_k$, this means that $\lambda(2^n-1) = \lambda(a_j)$. Consequently, $N(2^n-1) \geq N(a_j) + 1$. Also, the fact that there are no carries in $a_j + a_k$ implies that $\nu(2^n-1) = \nu(a_j) + \nu(a_k)$ by Lemma 1.

In the case $n = 16$ at least one of a_j or a_k must have at least five ones in its binary representation since $\nu(2^{16}-1) = 16$. In either event this means by Theorem C that $N(a_j) \geq 3$ which implies $N(2^{16}-1) \geq 4$. Thus, $l(2^{16}-1) \geq \lambda(2^{16}-1) + 4 = 15 + 4 = 16 + l(16) - 1$. To get an upper bound for $l(2^{16}-1)$ it needs first of all to be mentioned that a star chain is an addition chain where for each $i \geq 1$, $a_i = a_{i-1} + a_k$ for some $k \leq i - 1$. The minimal length of a star chain for an integer n is denoted by $l^*(n)$. Brauer [2] proved that the Scholz–Brauer conjecture is true if $l^*(n) = l(n)$, and Knuth has found that the first integer for which $l^*(n) > l(n)$ is 12509. Thus, the Scholz–Brauer conjecture holds true for the first 12508 positive integers. In particular it holds true for $n = 16$ from which it can be concluded that $l(2^{16}-1) = 16 + l(16) - 1$.

For $n = 17, 18, 20, 24$ and 32 it can easily be shown that $l(n) = 5$. In the step $2^n - 1 = a_j + a_k$ at least one of a_j or a_k has nine or more ones in its binary representation. In either event it can be concluded by [15, Theorem 1] that $N(a_j) \geq 4$, which means that $N(2^n-1) \geq 5$. Thus, in each of these five cases $l(2^n-1) \geq \lambda(2^n-1) + 5 = n + l(n) - 1$. On the other hand the Scholz–Brauer conjecture holds for each of these integers, and so it follows that $l(2^n-1) = n + l(n) - 1$.

Case $n = 15$ will now be considered. Since $l(15) = 5$, it is necessary to show that $N(2^{15}-1) \geq 5$. As in the other cases $N(2^{15}-1) \geq N(a_j) + 1$. If either a_j or a_k has nine or more ones in its binary representation, then $N(a_j) \geq 4$ by [15, Theorem 1], which implies $N(2^{15}-1) \geq 5$. It is possible, however, that $(\nu(a_j), \nu(a_k))$ is either $(8, 7)$ or $(7, 8)$. It must be shown in both of these cases that $N(a_j) \geq 4$. Propositions 1–4 of [15] will simplify this task and will be cited as needed.

It is clear from Theorem C that $N(a_j) \geq 3$ and $N(a_k) \geq 3$. If $\lambda(a_j) = \lambda(a_k) + m$ for some $m \geq 0$, then $N(a_j) \geq N(a_k) + 1 \geq 4$ by Lemma 3 unless $2^m a_k \geq a_j$. Therefore it will be assumed that $2^m a_k \geq a_j$. Also if $\lambda(a_j) = \lambda(a_k) + 1$, it will be assumed for the same reasons as in case (6, 5) of Proposition A that $a_j = a_k + a_t$ for some $t \leq k < j$. Otherwise, $N(a_j) \geq 4$. With these restrictions kept in mind four ways of starting the configuration a_j/a_k will be listed and analyzed.

$$\begin{array}{llrl} (1) & a_j & = & 101\text{--} \\ & +a_k & = & 10\text{--} \\ & 2^{15}-1 & = & 111\text{--} \end{array} \qquad \begin{array}{llrl} (2) & a_j & = & 100\text{--} \\ & +a_k & = & 11\text{--} \\ & 2^{15}-1 & = & 111\text{--} \end{array}$$

$$\begin{array}{llrl} (3) & a_j & = & 110\text{--} \\ & +a_k & = & 1\text{--} \\ & 2^{15}-1 & = & 111\text{--} \end{array} \qquad \begin{array}{llrl} (4) & a_j & = & 111\text{--} \\ & +a_k & = & \\ & 2^{15}-1 & = & 111\text{--}. \end{array}$$

In each of the configurations the remaining twelve slots will be either 1/0 or 0/1 slots. The reason for this is that there are no carries in $a_j + a_k$ and $2^{15} - 1$ consists of fifteen ones in its binary representation. Case (8, 7) will be considered first.

In (1) it can be assumed that $a_j = a_k + a_t$ for some $t \leq k < j$. If a_k is subtracted from a_j to obtain a_t, then $\nu(a_t) = 8$ by Lemma 2. Also, it can be observed that $\lambda(a_t) = \lambda(a_k)$. Further, since $\nu(a_j) = 8$ and $\nu(a_k) = 7$, it follows that $a_j \neq 2a_k$, which means that a_k and a_t are two distinct members of the chain. Thus, $N(a_k) \geq N(a_t) + 1 \geq 4$ which implies $N(a_j) \geq 4$.

In (2), $N(a_k) \geq 4$ by [15, propositions 1 and 3] unless $a_k = 11001\text{--}1111\text{--}$. As in (1) it can be assumed that $a_j = a_k + a_t$ for some $t \leq k < j$. Configuration (2) can now be developed further, and it will be looked at from a subtraction point of view.

$$\begin{array}{lrl} a_j & = & 100110\text{--}0000\text{--} \\ -a_k & = & 11001\text{--}1111\text{--} \\ a_t & = & 110\text{---}0001\text{--}. \end{array}$$

By Lemma 2, $\nu(a_t) = 8$, and by [15, Proposition 4], $N(a_t) \geq 4$ unless $a_t = 11\text{--}d\text{--}11\text{--}11\text{--}e\text{--}11\text{--}$ where d and e indicate the number of zeros between ones and $e = d$ or $e = d - 1$. Also, $N(a_k) \geq N(a_t) + 1 \geq 4$ by Lemma 3 unless $2a_t \geq a_k$. The only way to meet all of these requirements is with the following configuration:

$$\begin{array}{lrl} a_j & = & 100110110000111 \\ -a_k & = & 11001001111000 \\ a_t & = & 1101100001111. \end{array}$$

Again by the same reasoning as used in case (6, 5) of Proposition A, $N(a_k) \geq 4$ unless $a_k = a_t + a_s$ for some $s \leq t < k$. If a_t is subtracted from a_k to obtain a_s, it can be seen that $\nu(a_s) = 8$, $\lambda(a_k) = \lambda(a_t)$ and $a_k \neq a_t$. Thus, $N(a_t) \geq N(a_s) + 1 \geq 4$ which implies $N(a_j) \geq 4$.

In (3) it can be assumed that $2^2a_k \geq a_j$, which means that $a_k = 11\text{--}$. As in (2), $N(a_k) \geq 4$ unless $a_k = 11001\text{--}1111\text{--}$. The only way to meet both of these requirements is with the following configuration:

$$
\begin{aligned}
a_j &= 110011000001111\\
+a_k &= 1100111110000\\
2^{15}-1 &= 111111111111111.
\end{aligned}
$$

In this case $N(a_j) \geq 4$ by [15, Proposition 4].

In (4), $\lambda(a_j) = \lambda(a_k) + m$ for some $m \geq 0$. As has been mentioned it can be assumed that $2^m a_k \geq a_j$. This means $a_k = 111$--, and by [15, Proposition 1], $N(a_k) \geq 4$ which implies $N(a_j) \geq 4$.

Since $N(a_j) \geq 4$ in all four cases, it follows that $N(2^{15}-1) \geq 5$ in (8, 7). In case (7, 8) configurations (1) and (4) can be dispensed with in essentially the same manner as in (8, 7). The other two configurations will be considered.

In (2) it can be assumed as before that $a_j = a_k + a_t$ for some $t \leq k < j$. When a_k is subtracted from a_j to obtain a_t, then $\lambda(a_k) = \lambda(a_t) + m$ for some $m \geq 0$. By Lemma 2, $\nu(a_t) = 7$, and by Lemma 3, $N(a_k) \geq N(a_t) + 1 \geq 4$ unless $2^m a_t \geq a_k$. If this is the case, then $a_t = 11$--, and by Propositions 1 and 3, $N(a_t) \geq 4$ unless $a_t =$ 11001--1111--. The configuration a_j/a_k must then be as follows:

$$
\begin{aligned}
a_j &= 10011001\text{--}\\
-a_k &= 1100110\text{--}\\
a_t &= 11001\text{---}.
\end{aligned}
$$

In order that $2a_t \geq a_k$, it follows that $a_t = 1100111110000$. But it is impossible to obtain a_t in this form since a one will appear in a_t at the extreme right of a_j/a_k regardless of whether there is a 1/0 slot or a 0/1 slot in this place. Thus, $N(a_j) \geq 4$ in any event.

In (3) since $\nu(a_j) = 7$ and $a_j = 110$--, it can be assumed that $a_j =$ 11001--1111--. Also, it can be assumed that $2^2 a_k \geq a_j$, which means that $a_k = 11$--. Since $\nu(a_k) = 8$, $N(a_k) \geq 4$ by Propositions 2 and 4 unless $a_k = 11$--d--11--11--e--11-- where $e = d$ or $e = d - 1$. If $2^2 a_k \geq a_j$, then $d \leq 2$. With these restrictions there are two possibilities for a_j/a_k :

(3a)
$$
\begin{aligned}
a_j &= 110010011110000\\
+a_k &= 1101100001111\\
2^{15}-1 &= 111111111111111
\end{aligned}
$$

(3b)
$$
\begin{aligned}
a_j &= 110010000001111\\
+a_k &= 1101111110000\\
2^{15}-1 &= 111111111111111.
\end{aligned}
$$

In both cases $\lambda(a_j) = \lambda(a_k) + 2$ while $a_j > 2a_k + a_k$. By Lemma 4, $N(a_j) \geq N(a_k) + 1 \geq 4$ unless $a_j = 2a_{k+1}$. This is impossible in (3b) since a_j is odd. In (3a), $\lambda(a_{k+1}) = \lambda(a_k) + 1$, and $\nu(a_{k+1}) = 7$. By the same reasoning as used before, it can be assumed that $a_{k+1} = a_k + a_t$ for some $t \leq k < k+1$. Since $a_j = 2a_{k+1}$, the binary form of a_{k+1} is the same as that of a_j except that all the digits are shifted to the right one place. Configuration a_{k+1}/a_k is as follows:

$$
\begin{aligned}
a_{k+1} &= 11001001111000\\
-a_k &= 1101100001111\\
a_t &= 1011101101001.
\end{aligned}
$$

As can be seen $N(a_k) \geq N(a_t) + 1 \geq 4$. Thus, $N(a_j) \geq 4$.

In all possibilities $N(a_j) \geq 4$, which implies $N(2^{15} - 1) \geq 5$. It can be concluded that $l(2^{15} - 1) \geq \lambda(2^{15} - 1) + 5 = 15 + l(15) - 1$. Since the Scholz–Brauer conjecture holds for $n = 15$, it follows that $l(2^{15} - 1) = 15 + l(15) - 1$. This now gives the following theorem.

Theorem 2. $l(2^n - 1) = n + l(n) - 1$ *for the first eighteen positive integers n and for* $n = 20$, 24 *and* 32.

It seems too bold to conjecture that equality holds for all positive integers n. This question, of course, is at least as difficult as establishing the Scholz–Bauer conjecture itself. It even may be somewhat difficult to find further values of n for which equality can be shown to hold.

Recently, Schönhage [11] has proved the fine result that $l(n) \geq \log_2 n + \log_2 \nu(n) - 2.13$. This improves the result of Cottrell [3] that $l(n) \geq \log_2 n + \log_2 \nu(n) - 1$ and comes close to establishing the validity of a conjecture by Stolarsky [12] that $\nu(n) \leq 2^{l(n)-\lambda(n)}$. Unfortunately, it does not appear that Schönhage's result will shorten this paper. Even if $\nu(n) \leq 2^{l(n)-\lambda(n)}$, it needs to be shown that $\nu(n) \leq 2^{l(n)-\lambda(n)-1}$ for the integers for which $l(2n) = l(n)$. A slightly weaker form of Stolarsky's conjecture is that $l(n) \geq \log_2 n + \log_2 \nu(n) - 1$. If this is true then it is not hard to show that there are infinite classes of integers n for which $l(2^n - 1) = n + l(n) - 1$. For instance, this equality would be satisfied by those integers n with one or two ones in their binary representation.

References

[1] R.E. Bellman, Advanced problem 5125, Amer. Math. Monthly 70 (1965) 765.

[2] A.T. Brauer, On addition chains, Amer. Math. Soc. 45 (1939) 736–739.

[3] A. Cottrell, A lower bound for the Scholz–Brauer problem, Notices Amer. Math. Soc. 20 (1973) A-476.

[4] P. Erdös, Remarks on number theory III on addition chains, Acta Arith. 6 (1960) 77–81.

[5] A.A. Gioia, M.V. Subbarao and M. Sugunumma, The Scholz–Brauer problem in addition chains, Duke Math. J. 29 (1962) 481–487.

[6] W. Hansen, Zum Scholz–Brauerchen Problem, J. Reine Angew. Math. 202 (1959) 129–136.

[7] A.M. Il'in, On additive number chains, Problemy Kibernet. 13 (1965) 245–248.

[8] H. Kato, On addition chains, Ph.D. Dissertation, University of Southern California, Los Angeles, CA (June 1970).

[9] D.E. Knuth, The Art of Computer Programming, Vol. 2 (Addison-Wesley, Reading, Mass., 1969) 398–422.

[10] A. Scholz, Jahresbericht, Deutsche Math.-Verein. 47 (1937) 41.

[11] A. Schönhage, Eine untere Schranke für die Lange von Additionsketten, Mathematisches Institut der Universität, Tübingen, West Germany, in preparation.

[12] K.B. Stolarsky, A lower bound for the Scholz–Brauer problem, Can. J. Math. 21 (1969) 675–683.

[13] E.G. Straus, Addition chains of vectors, Amer. Math. Monthly 71 (1964) 806–808.

[14] E.G. Thurber, The Scholz–Brauer problem on addition chains, Ph.D. Dissertation, University of Southern California, Los Angeles, CA (September 1971).

[15] E.G. Thurber, The Scholz-Brauer problem on addition chains, Pacific J. Math. 49 (1973) 229–242.
[16] E.G. Thurber, On addition chains $l(mn) \leq l(n) - b$ and lower bounds for $c(r)$, Duke Math. J. 40 (1973) 907–913.
[17] W.R. Utz, A note on the Scholz-Brauer problem on addition chains, Proc. Amer. Math. Soc. 4 (1953) 462–463.
[18] C.T. Whyburn, A note on addition chains, Proc. Amer. Math. Soc. 16 (1965) 1134.