ON ADDITION CHAINS

ALFRED BRAUER

We consider a set $a_0 = 1 < a_1 < a_2 < \cdots < a_r = n$ of integers such that every element a_ρ can be written as sum $a_\sigma + a_\tau$ of preceding elements of the set. Such sets of integers have been called "addition chains (Additionsketten) for n" by A. Scholz.† For example, for $n = 666$,

$$1, 2, 4, 8, 16, 24, 40, 80, 160, 320, 640, 664, 666$$

forms an addition chain with $r = 12$; the same holds for

$$1, 2, 3, 6, 9, 18, 27, 54, 81, 162, 324, 648, 666.$$

In any case, we must have $a_1 = 2$ and $a_2 = 3$ or 4.

By the length $l = l(n)$ of n, Scholz understands the smallest l for which there exists an addition chain $a_0, a_1, \cdots, a_l = n$.

The following question leads to addition chains: The least positive residue of $c^n \pmod{m}$ (c, m, n given integers) is to be formed using the smallest possible number of multiplications. Then $l(n)$ multiplications will always suffice.

A. Scholz published the following inequalities for $l(n)$ in the form of problems:

$$m + 1 \leqq l(n) \leqq 2m \quad \text{for} \quad 2^m + 1 \leqq n \leqq 2^{m+1}, \qquad m \geqq 1, \tag{1}$$

$$l(ab) \leqq l(a) + l(b). \tag{2}$$

In (1), we have $l(n) < 2m$ whenever $m > 2$; moreover,

$$l(2^{m+1} - 1) \leqq m + l(m + 1). \tag{3}$$

In connection with (3), Scholz surmises that (1) can be improved generally. He further raises the question of whether or not the inequality

$$1 \leqq \limsup_{n \to \infty} \frac{\log 2}{\log n} l(n) \leqq 2, \tag{4}$$

which easily follows from (1), can be improved.

It is easy to prove the formulas (1) and (2). I cannot decide whether (3) is always true. In the following, I will show that

$$l(2^{m+1} - 1) \leqq m + l^*(m + 1),$$

† Jahresbericht der deutschen Mathematiker-Vereinigung, class II, vol. 47 (1937), p. 41.

where $l^*(m+1)$ is the minimal length, not of all, but only of certain addition chains. Further, I will prove by elementary methods that for sufficiently large n

$$l(n) < \frac{\log n}{\log 2}\left\{1 + \frac{1}{\log\log n} + \frac{2\log 2}{(\log n)^{1-\log 2}}\right\}.$$

This is better than (1). It entails the following relation

$$\lim_{n\to\infty} \frac{\log 2}{\log n}\, l(n) = 1,$$

which, of course, is better than (4).

Let $a_0, a_1, \cdots, a_l = n$ be an addition chain for n, $2^m+1 \leqq n \leqq 2^{m+1}$. Then $a_\lambda \leqq 2a_{\lambda-1}$, $(\lambda = 1, 2, \cdots, l)$. Since $a_1 = 2$, we have $a_l \leqq 2^l$, $n \leqq 2^l$, $2^m+1 \leqq 2^l$, $m+1 \leqq l$. This proves the first half of (1).

To prove the second part of (1), $l(n) \leqq 2m$, suppose first that $2^m+1 \leqq n < 2^{m+1}$. We write n as a binary number

$$n = 2^{\nu_1} + 2^{\nu_2} + \cdots + 2^{\nu_k}, \quad \nu_1 < \nu_2 < \cdots < \nu_k.$$

We have here at most $m+1$ terms, $k \leqq m+1$, and $\nu_k = m$. We begin the addition chain with $a_0 = 1$, $a_1 = 2$, $a_2 = 4$, $\cdots$, $a_m = 2^m$, and take then

$$a_{m+1} = 2^m + 2^{\nu_1}, \; a_{m+2} = 2^m + 2^{\nu_1} + 2^{\nu_2}, \cdots,$$
$$a_{m+k-1} = 2^m + 2^{\nu_1} + \cdots + 2^{\nu_{k-1}} = n.$$

This actually is an addition chain, and we see that $l(n) \leqq m+k-1 \leqq 2m$. The equality $l(n) = 2m$ is possible only if $k = m+1$,

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

This case will be discussed in the last paragraph of this page.

For $n = 2^{m+1}$, we form the addition chain

$$(5) \qquad 1, 2, 2^2, \cdots, 2^{m+1}.$$

Here $l = m+1$, hence $l(2^{m+1}) = m+1 \leqq 2m$.

Let $1, a_1, a_2, \cdots, a_r = a$ be an addition chain for a with $r = l(a)$, and let $1, b_1, b_2, \cdots, b_s$ be one for b with $s = l(b)$. Then

$$1, a_1, \cdots, a_r, a_rb_1, a_rb_2, \cdots, a_rb_s$$

forms an addition chain for $a_rb_s = ab$, since $b_\rho = b_\sigma + b_\tau$ implies $a_rb_\rho = a_rb_\sigma + a_rb_\tau$. The number of terms after 1 in this chain is $r+s$; hence $l(ab) \leqq r+s = l(a)+l(b)$. This proves (2).

By a special addition chain for the number n we mean an addition chain for which, for all ρ, and for some σ

$$a_\rho = a_{\rho-1} + a_\sigma, \qquad 0 \leqq \sigma \leqq \rho - 1 \leqq l - 1,$$

holds. Let $l^*(n)$ be the minimal length of all special addition chains for n. Then $l(n) \leqq l^*(n)$. The chains used in the proof of the second part of (1) are special chains. Hence, it follows from this proof that $l^*(n) \leqq 2m$. The equality sign is here impossible except for $n = 2^{m+1} - 1$. In order to prove that $l(n) < 2m$ whenever $m > 2$, it suffices to show that

$$l(2^{m+1} - 1) \leqq l^*(2^{m+1} - 1) \leqq m + l^*(m + 1), \tag{6}$$

for 1, 2, 4, 5, 6, 7, $\cdots$, $m+1$ is a special chain of length $m-1$ for $m+1$, so $l^*(m+1) \leqq m-1$. Let

$$1 = a_0, a_1, \cdots, a_k = m + 1 \tag{7}$$

be a minimal special addition chain for $m+1$, $k = l^*(m+1)$. We form

$$2^{a_0} - 1 = 1,\ 2^{a_1} - 1 = 3,\ 2^{a_2} - 1, \cdots, 2^{a_k} - 1$$

and multiply $2^{a_\kappa} - 1$ successively $a_{\kappa+1} - a_\kappa$ times by 2, $(\kappa = 0, 1, 2, \cdots, k-1)$. We then obtain

$$(a_1 - a_0) + (a_2 - a_1) + \cdots + (a_k - a_{k-1}) = m$$

further numbers. We thus obtain the integers

$$\begin{aligned} &1, 2, 2^{a_1} - 1, 2(2^{a_1} - 1), 2^2(2^{a_1} - 1), \cdots, 2^{a_2-a_1}(2^{a_1} - 1), 2^{a_2} - 1, \\ &2(2^{a_2} - 1), \cdots, 2^{a_3-a_2}(2^{a_2} - 1), \cdots, 2^{a_k-a_{k-1}}(2^{a_{k-1}} - 1), 2^{a_k} - 1. \end{aligned} \tag{8}$$

We state that these numbers form a special chain for $2^{a_k} - 1 = 2^{m+1} - 1$. This will be proved if we show that

$$2^{a_\kappa} - 1 - 2^{a_\kappa - a_{\kappa-1}}(2^{a_{\kappa-1}} - 1) = 2^{a_\kappa - a_{\kappa-1}} - 1$$

is an element of (8) for $\kappa = 2, 3, \cdots, k$. But this is true, since (7), as a special addition chain, contains $a_\kappa - a_{\kappa-1}$. The length of the chain (8) is $k + m = l^*(m+1) + m$, and this proves (6).

We show now that A. Scholz' conjecture, that (1) and (4) can be improved, is actually true. We prove the following theorem:

THEOREM. *If r is any positive and s any not negative integer, then*

$$l(n) \leqq (r + 1)s + 2^r - 2 \quad \textit{for} \quad 2^{rs} \leqq n < 2^{r(s+1)}. \tag{9}$$

PROOF. When $r = 1$, this follows from (1); we therefore take $r > 1$ and fixed. I state now that we can form an addition chain for n which contains at most $(r+1)s + 2^r - 2$ terms, and which begins with the terms $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $\cdots$, $a_{2^r-2} = 2^r - 1$. For $s = 0$ this is true because the integers 1, 2, $\cdots$, $2^r - 1$ form an addition chain for every

$n<2^r$ (the integers $n+1$, $n+2, \cdots, 2^r-1$ may be included in the chain). Assume now that the assertion is not true and take s to be the smallest value for which the statement does not hold for n with $2^{rs} \leqq n < 2^{r(s+1)}$. We divide n by 2^r:

$$n = a \cdot 2^r + b, \qquad 0 \leqq b < 2^r. \tag{10}$$

Then $2^{r(s-1)} \leqq a < 2^{rs}$, and since our statement is supposed to be true for $s-1$ instead of s, there exists an addition chain $a_0, a_1, a_2, \cdots, a_{\alpha-1}, a_\alpha = a$ for a which has at most $(r+1)(s-1)+2^r-2$ terms, and which starts with $1, 2, \cdots, 2^r-1$. Because of (10), this chain contains b for $b>0$. Then $a_0, a_1, \cdots, a_{\alpha-1}, a, 2a, 2^2a, \cdots, 2^ra, 2^ra+b$ is an addition chain for n which contains the first 2^r-1 integers. The length equals at most

$$(r + 1)(s - 1) + 2^r - 2 + r + 1 = (r + 1)s + 2^r - 2.$$

This gives the desired contradiction; therefore the statement holds for all values of s. The proof yields an easy method for constructing the addition chains.

From relation (9) it follows that $s \leqq (\log n)/r \cdot \log 2$; hence $l(n) \leqq (r+1)(\log n)/(r \log 2)+2^r-2$. If now $2^m \leqq n < 2^{m+1}$, this yields

$$l(n) \leqq \min_{r=1,2,\cdots,m} \left\{\left(1 + \frac{1}{r}\right)\frac{\log n}{\log 2} + 2^r - 2\right\}. \tag{11}$$

For instance, if we set $r = [\log \log n]+1$ for $n \geqq 3$, then (11) gives

$$\begin{aligned} l(n) &< \left(1 + \frac{1}{\log\log n}\right)\frac{\log n}{\log 2} + 2^{\log\log n + 1} \\ &= \left(1 + \frac{1}{\log\log n}\right)\frac{\log n}{\log 2} + 2e^{\log\log n \cdot \log 2} \\ &= \frac{\log n}{\log 2}\left(1 + \frac{1}{\log\log n}\right) + 2(\log n)^{\log 2}, \end{aligned}$$

$$l(n) < \frac{\log n}{\log 2}\left\{1 + \frac{1}{\log\log n} + \frac{2\log 2}{(\log n)^{1-\log 2}}\right\}. \tag{12}$$

This inequality can easily be improved since the expression between the braces in (11) takes on its minimum for $r^2 \cdot 2^r = (\log n)/(\log 2)^2$.

On the other hand, it follows from (1) that $l(n) \geqq m > (\log n)/(\log 2) - 1$. This, in connection with (12) yields $\lim_{n\to\infty} l(n)(\log 2)/(\log n) = 1$.

THE INSTITUTE FOR ADVANCED STUDY