STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

ZW 1968-001

Efficient Calculation of Powers in a Semigroup

by

E. Wattel

and

G.A. Jensen

February 1968

The Mathematical Centre at Amsterdam, founded the 11th of February, 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

§1. Introduction and notation

This report deals with a problem related to some results of A. Scholz [3] concerning "addition chains". An addition chain for a natural number n is a finite ordered set of natural numbers $n_0, n_1, \ldots, n_k$ such that $n_0 = 1$, $n_k = n$ and every number of the chain except n_0 is the sum of two preceding members of the chain. Obviously for such a chain, $n_1 = 2$ and n_2 is either 3 or 4.

The problem of constructing addition chains for a natural number n is related to the following problem [c.f. 1]:
If a is an arbitrary element of a semigroup, what is the minimal number of multiplications necessary to compute a^n from a? If $n_0, \ldots, n_k$ is an addition chain for n, then we can form the set $a = a^{n_0}, a^{n_1}, \ldots, a^{n_k} = a^n$. Each number of this set is the product of two preceding ones and the number k gives the member of multiplications which is necessary to compute a^n from a by means of this chain. In general k need not be the smallest number of multiplications necessary to compute a^n from a.

Let $\mathcal{C}_n$ be the collection of all addition chains for n. If $C \in \mathcal{C}_n$, let $\lambda(C)$ be the number of elements in the chain minus one. We will also say that $\lambda(C)$ is the length of C and we note that $\lambda(C)$ is precisely the number of multiplications which is necessary to compute a^n from a by means of the chain C. We also let

$$\lambda(n) = \min\{\lambda(C) \mid C \in \mathcal{C}_n\},$$

and note that $\lambda(n)$ is the minimum number of multiplications which is necessary to compute a^n from a.

Some obvious consequences of the above definitions are that $\lambda(1) = 0$, $\lambda(2) = 1$, $\lambda(3) = 2$, and $\lambda(4) = 2$.

A Brauer [2] and E.G. Strauss [4] have proved that

$$\lim_{n\to\infty} \frac{\lambda(n)}{\log_2 n} = 1$$

and

$$\lambda(n) \leq \frac{\ln (n)}{\ln (2)} \{1 + O(\frac{1}{\ln \ln n})\}.$$

Moreover, Scholtz has stated in [3] that

$$\lambda(n) \geq \log_2 n.$$

From these results, it is obvious that there exists a natural number n for which $\frac{\lambda(n)}{\log_2 n}$ is a maximum. One of the main purposes of this report is to prove that the function is a maximum for n = 71, where $\lambda(n) = 9$ and $\frac{\lambda(n)}{\log_2 n} = 1{,}463\ldots$. However, we also compute $\lambda(n)$ for several numbers n and techniques for computing upper bounds for $\lambda(n)$ are given.

In the second section we prove some elementary inequalities for $\lambda(n)$ and use these inequalities to show that if n is a number for which $\frac{\lambda(n)}{\log_2 n}$ is a maximum, then there exists a prime p such that $\frac{\lambda(p)}{\log_2 p} = \frac{\lambda(n)}{\log_2 n}$.

In the third section Brauer's techniques are modified in order to prove a theorem which yields a sharper result than Brauer's inequality (12). Special cases of the theorem which are necessary for section 5 are also discussed.

The main content of section 4 is two tables which are needed for the proof of the main theorem. A proof for some of the entries in table 1 is contained in the appendix.

The last section of the report contains a proof that $\frac{\lambda(n)}{\log_2 n}$ is a maximum for n = 71.

We wish to express our gratitude to the members of the department of pure mathematics of the Mathematical Centre and to F. Göbel for their discussion and comments during the research for this report.

§2. Elementary inequalities.

2.1. Proposition. For every natural number n,

$$\frac{\lambda(n)}{\log_2 n} \geq 1.$$

Proof. It is clear that $\max\{n \mid \lambda(n) \leq 1\} = 2$. Suppose now that for some natural number k we have shown that $\max\{n \mid \lambda(n) \leq k\} = 2^k$. Let m be a natural number such that $\lambda(m) \leq k+1$ and let $C \in \mathcal{C}_m$ such that

$\lambda(C) = \lambda(m)$. If we delete the last term from the chain C, we have a chain whose length is at most k and by our induction assumption, all of these terms are less than or equal to 2^k. Since the last term of C is the sum of two preceding terms, it follows that the last term of C is less than or equal to 2^{k+1}. Moreover, equality holds only if 2^k belongs to C. Thus $\max \{n|\lambda(n) \leq k + 1\} = 2^{k+1}$ holds for every integer $k \geq 0$. It follows easily that $\lambda(n) \geq \log_2 n$ and so $\frac{\lambda(n)}{\log_2 n} \geq 1$.

2.2. Proposition. Let r, s, n be natural numbers such that n = rs. Then

$$\lambda(n) \leq \lambda(r) + \lambda(s).$$

Moreover, for any natural number n,

$$\lambda(n+1) \leq \lambda(n) + 1 \text{ and } \lambda(n+2) \leq \lambda(n) + 1.$$

Proof. In order to prove the first assertion, let $k = \lambda(r)$, let $l = \lambda(s)$, assume $r_0, \ldots, r_k$ is an addition chain for r and assume $s_0, \ldots, s_l$ is an addition chain for s. We define an addition chain for n as follows:

$$n_i = \begin{cases} r_i & i \leq k, \\ rs_{i-k} & k \leq i \leq k+l. \end{cases}$$

The length of this addition chain is k + l and so

$$\lambda(n) \leq k + l = \lambda(r) + \lambda(s).$$

The second and third assertions are easy consequences of the fact that every addition chain starts with the numbers 1 and 2; hence any chain which ends with n can be extended to a chain ending with n + 1 or n + 2 with only one extra addition.

2.3. Corollary. If n = rs, then

$$\frac{\lambda(n)}{\log_2 n} \leq \max\left\{\frac{\lambda(r)}{\log_2 r}, \frac{\lambda(s)}{\log_2 s}\right\}.$$

Proof. Since $\lambda(n) \leq \lambda(r) + \lambda(s)$, then

$$\frac{\lambda(n)}{\log_2 n} \leq \frac{\lambda(r) + \lambda(s)}{\log_2 n} = \frac{\lambda(r) + \lambda(s)}{\log_2 r + \log_2 s} \leq \max\left\{\frac{\lambda(r)}{\log_2 r}, \frac{\lambda(s)}{\log_2 s}\right\}.$$

2.4. Corollary. If n is a natural number such that $\frac{\lambda(n)}{\log_2 n}$ is a maximum, then there exists a prime $p \leq n$ such that $\frac{\lambda(p)}{\log_2 p} = \frac{\lambda(n)}{\log_2 n}$; in this case, n is a power of p.

Proof. It follows from the preceding corollary that

$$\frac{\lambda(n)}{\log_2 n} \leq \max\{\frac{\lambda(p)}{\log_2 p} | p \text{ is a prime divisor of } n\}.$$

On the other hand, $\frac{\lambda(n)}{\log_2 n} \geq \frac{\lambda(p)}{\log_2 p}$ for every prime p so that there must exist a prime divisor p of n for which $\frac{\lambda(n)}{\log_2 n} = \frac{\lambda(p)}{\log_2 p}$. It follows easily that $n^{\lambda(p)} = p^{\lambda(n)}$ and hence n is a power of p. Clearly, this prime p must be unique.

§3. Upper bounds for $\lambda(n)$.

The proof of the following theorem essentially uses the techniques of Brauer [2]. One of its applications is to obtain a sharper result than Brauer's inequality (12).

3.1. Theorem. Let n and k be two natural numbers such that $n \geq 2^{2k}$. Then

$$\lambda(n) \leq [\log_2 n] + \left[\frac{\log_2 n}{k}\right] - k + 2^{k-1} + 1.$$

Proof. Let

$$\varepsilon_l \varepsilon_{l-1} \cdots \varepsilon_1 \varepsilon_0, \qquad (\varepsilon_l = 1 \text{ and } \varepsilon \in \{0, 1\})$$

be the binary representation of n and let $t = \left[\frac{l}{k}\right]$. The method of proof for the theorem is as follows: We first construct an initial addition chain. By doubling previous terms and adding members of the initial chain to terms, we compute the maximum number of terms that are needed for an addition chain to contain the following numbers:

$$\varepsilon_l \varepsilon_{l-1} \cdots \varepsilon_{l-k+1}0,\ \varepsilon_l \varepsilon_{l-1} \cdots \varepsilon_{l-k+1}\varepsilon_{l-k} \cdots \varepsilon_{l-2k+1},\ \cdots,\ \varepsilon_l \varepsilon_{l-1} \cdots \varepsilon_1 \varepsilon_0.$$

To illustrate our method, we first consider the following example.

Example. Let n be the natural number whose binary representation is 100 101 110 111 01 and let k = 3. It follows that l = 13 and

$\left[\frac{l}{k}\right] = 4$. We break the number up into 4 blocks of length 3 with a block of length 2 left over; i.e. 100, 101, 110, 111, and 01. Our initial chain (in binary notation) is

$$n_0 = 1, \quad n_1 = 10, \quad n_2 = 11, \quad n_3 = 101, \text{ and } n_4 = 111.$$

The next number that we consider is 1000. It is sum of two members of the initial chain; namely $n_4 + n_0$. We also note that the number 101 is also in the initial addition chain. Thus, the next 4 members of the addition chain are formed as follows:

$$n_5 = n_4 + n_0 = 1000, \quad n_6 = n_5 + n_5 = 10000,$$

$$n_7 = n_6 + n_6 = 100000, \text{ and } n_8 = n_7 + n_3 = 100101.$$

In the next step, we examine the number 110. It is not in the initial chain but 11 is. Hence the next 4 members of the chain are formed as follows:

$$n_9 = n_8 + n_8 = 1001010, \quad n_{10} = n_9 + n_9 = 10010100,$$

$$n_{11} = n_{10} + n_2 = 10010111, \text{ and } n_{12} = n_{11} + n_{11} = 100101110.$$

Continuing, we note that 111 is in the initial chain and so the next 4 terms are defined by:

$$n_{13} = n_{12} + n_{12}, \quad n_{14} = n_{13} + n_{13}, \quad n_{15} = n_{14} + n_{14}, \text{ and}$$

$$n_{16} = n_{15} + n_4 = 100101110111.$$

Finally, since 01 is in the initial chain, let $n_{17} = n_{16} + n_{16}$, $n_{18} = n_{17} + n_{17}$, and $n_{19} = n_{18} + n_0 = 10010111011101$. Thus we have an addition chain of length

$$19 = 2^{3-1} + (4-1)(3+1) + (13-12+2).$$

Proof of the theorem.

Step 1. Let the initial addition chain be

$$1, 10, 11, 101, 111, \ldots, \overbrace{111 \ldots 1}^{k \text{ times}}$$

There are precisely 2^{k-1} members of this chain since it contains all of the odd numbers between 1 and 2^k.

Step 2. The numbers $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-k+1}0$ can be written as the sum of two members of the initial chain, namely the last term plus some other term. Thus we let it be the next term of the addition chain. Next we consider the number

$$\varepsilon_{l-k}\varepsilon_{l-k-1} \cdots \varepsilon_{l-2k+1}.$$

Either $\varepsilon_{l-k} = \varepsilon_{l-k-1} = \cdots = \varepsilon_{l-2k+1} = 0$ or there exists a least index i such that $\varepsilon_i = 1$ and $l-k \geq i \geq l-2k+1$. In the former case by doubling $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-k+1}0$ and then doubling the obtained number, etc., we can construct the number $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-2k+1}$ in k steps beyond the initial chain. In the latter case, the number $\varepsilon_{l-k}\varepsilon_{l-k+1} \cdots \varepsilon_{i+1}\varepsilon_i$ belongs to the initial addition chain (since it is the representation of an odd number less than 2^k). In this case we double $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-k+1}0$ and then double the obtained number and repeat this procedure exactly l-k-i times. Then we add $\varepsilon_{l-k}\varepsilon_{l-k-1} \cdots \varepsilon_i$ to the last number we obtained and repeat the doubling process exactly $i - (l-2k+1)$ times in order to obtain the number $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-2k+1}$. Thus it takes

$$1 + (l-k-i) + 1 + i - (l-2k+1) = k+1$$

additional terms to construct $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-2k+1}$ from the initial chain.

Step 3. Suppose that we have constructed an addition chain for $\varepsilon_l\varepsilon_l \cdots \varepsilon_{l-rk+1}$. We compute the maximum number of terms necessary to construct an addition chain for $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-(r+1)k+1}$ using the addition chain for $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-rk+1}$. As in step 2, either $\varepsilon_{l-rk} = \varepsilon_{l-rk-1} = \cdots = \varepsilon_{l-(r+1)k+1} = 0$ or there is a least index i such that $\varepsilon_i = 1$ and $l-rk \geq i \geq l-(r+1)k+1$. In the former case we use the doubling process to obtain an addition chain for $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-(r+1)k+1}$ in just k steps from $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-rk+1}$. In the second case we proceed as in step 2 by using the doubling process exactly l-rk+i+1 times, adding $\varepsilon_{l-rk}\varepsilon_{l-rk+1} \cdots \varepsilon_i$, and then doing the doubling process $i-l+(r+1)k-1$ more times. In this case we obtain $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-(r+1)k+1}$ in k+1 additional steps from $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-rk+1}$.

Step 4. Since we can construct an addition chain for $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-tk+1}$ by step 3, we need only compute the maximum number of steps necessary to construct an addition chain for $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_1\varepsilon_0$ using the addition chain for $\varepsilon_l\varepsilon_{l-1} \cdots \varepsilon_{l-tk+1}$. We use the methods of steps 2 and 3 and note that it will take l-tk+1 of the doubling steps plus at most one addition from the initial chain. Thus there are at most l-tk+2 additional terms necessary for the chain.

Step 5. We can now add up the maximum number of terms from each step. There are 2^{k-1} terms from step 1, at most k+1 terms from step 2, at most (t-2)(k+1) terms from step 3, and at most l-tk+2 terms from step 4. Thus the maximum number of terms that we have is

$$2^{k-1} + (t-1)(k+1) + l - tk + 2 = 2^{k-1} + l + t - k + 1.$$

If we observe that $t = \left[\frac{l}{k}\right]$ and $l = \lceil \log_2 n \rceil$, then

$$\lambda(n) \leq \lceil \log_2 n \rceil + \left[\frac{\log_2 n}{k}\right] + 2^{k-1} - k + 1.$$

The theorem is also valid if $k < 2^{2n}$, however, such a result is not needed in this report and so a proof is not included.

Using the theorem, we are able to find an upper bound for the order of $\lambda(n)$. For n sufficiently large, we put

$$k = \lceil \log_2 \log_2 n - 2\log_2 \log_2 \log_2 n + 2 \rceil.$$

It follows that

$$2^{k-1} \leq \frac{2\log_2 n}{(\log_2 \log_2 n)^2} \quad \text{and} \quad \left[\frac{\log_2 n}{k}\right] \leq \frac{\log_2 n}{\log_2 \log_2 n - 2\log_2 \log_2 \log_2 n}.$$

Thus

$$\frac{\lambda(n)}{\log_2 n} \leq 1 + \frac{1}{\log_2 \log_2 n - 2\log_2 \log_2 \log_2 n} + \frac{2}{(\log_2 \log_2 n)^2} + 1 - \frac{k}{\log_2 n}$$

and hence

$$\frac{\lambda(n)}{\log_2 n} \leq 1 + \frac{1}{\log_2 \log_2 n} + o\left(\frac{1}{\log_2 \log_2 n}\right).$$

This result is sharper than Brauer's inequality (12).

For the proof in section 5, we consider upperbounds for $\lambda(n)$ in

case k = 2 or k = 3. For convenience, we denote the smallest integer which is not smaller than a by $\lceil a \rceil^+$.

The case for which k = 2. The initial chain in this case is 1, 10, 11 (in binary notation). If n is any natural number which is larger than 3, then all possible first three digits for the binary representation of n are 100, 101, 110, and 111. In case the first three digits are 100, 101 or 110, then we can obtain the first three digits in three additions. If l is the number of digits needed to represent n in the binary system, then we need at most l-3 doublings and $\left\lceil \frac{l-3}{2} \right\rceil^+$ additions more to form a chain for n. Since $l = \lceil \log_2 n \rceil^+$ if n is not a power of 2, then it follows that in this case

$$\lambda(n) \leq \lceil \log_2 n \rceil^+ + \left\lceil \frac{\log_2 n - 3}{2} \right\rceil^+ . \tag{3.2}$$

In the case that the first three digits of the representation of n are 111, then we have the first two digits in two additions and we see that

$$\lambda(n) \leq \lceil \log_2 n \rceil^+ + \left\lceil \frac{\log_2 n - 2}{2} \right\rceil^+ . \tag{3.3}$$

Clearly both (3.3) and (3.4) hold if n is a power of 2.

The case for which k=3. The initial chain for this case is 1, 10, 11, 101, 111 (in binary notation). Let n be a natural number which is larger than 7. If the first four digits of the binary representation of n are 1000, 1001, 1010, 1100 or 1110, then it is possible to make these digits in five steps. As before, we still need at most $l-4+\left\lceil \frac{l-4}{3} \right\rceil^+$ more steps for an addition chain for n, where l is the number of digits needed to represent n in the binary system. Thus in this case

$$\lambda(n) \leq 5 + (l-4) + \left\lceil \frac{l-4}{3} \right\rceil^+ = \lceil \log_2 n \rceil^+ + \left\lceil \frac{\log_2 n - 1}{3} \right\rceil^+ . \tag{3.4}$$

If the first four digits are 1011, 1101, or 1111, then we have the first three digits and an extra 0 in five steps.

Hence

$$\lambda(n) \leq 5 + (l-4) + \left\lceil \frac{l-3}{3} \right\rceil^+ = \lceil \log_2 n \rceil^+ + \left\lceil \frac{\log_2 n}{3} \right\rceil^+ \tag{3.5}$$

§4. Tables of $\lambda(n)$ and $(71)^{\frac{m}{q}}$

In order to illustrate the behavior of $\lambda(n)$, we include a table of $\lambda(n)$ for $n \leq 100$. For a discussion of this table, see the appendix.

n	$\lambda(n)$	n	$\lambda(n)$	n	$\lambda(n)$	n	$\lambda(n)$
1	0	26	6	51	7	76	8
2	1	27	6	52	7	77	8
3	2	28	6	53	8	78	8
4	2	29	7	54	7	79	9
5	3	30	6	55	8	80	7
6	3	31	7	56	7	81	8
7	4	32	5	57	8	82	8
8	3	33	6	58	8	83	8
9	4	34	6	59	8	84	8
10	4	35	7	60	7	85	8
11	5	36	6	61	8	86	8
12	4	37	7	62	8	87	9
13	5	38	7	63	8	88	8
14	5	39	7	64	6	89	9
15	5	40	6	65	7	90	8
16	4	41	7	66	7	91	9
17	5	42	7	67	8	92	8
18	5	43	7	68	7	93	9
19	6	44	7	69	8	94	9
20	5	45	7	70	8	95	9
21	6	46	7	71	9	96	7
22	6	47	8	72	7	97	8
23	6	48	6	73	8	98	8
24	5	49	7	74	8	99	8
25	6	50	7	75	8	100	8

table 1

In order to prove that $\frac{\lambda(n)}{\log_2 n}$ is maximal for n = 71, then for each natural number n we must construct an addition chain C such that $\frac{\lambda(C)}{\log_2 n} < \frac{\lambda(71)}{\log_2 71}$. From table 1 we see that $\lambda(71) = 9$ and so the last inequality is possible if and only if $n^9 > (71)^{\lambda(C)}$. This holds if and only if $n > (71)^{\frac{\lambda(C)}{9}}$. We include a table of $(71)^{\frac{m}{9}}$ for $1 \leq m \leq 20$.

m	$(71)^{\frac{m}{9}}$	m	$(71)^{\frac{m}{9}}$	m	$(71)^{\frac{m}{9}}$	m	$(71)^{\frac{m}{9}}$
1	1.61	6	17.15	11	183.08	16	1954.91
2	2.58	7	27.53	12	294.00	17	3139.22
3	4.14	8	44.21	13	472.11	18	5041.00
4	6.65	9	71.00	14	758.12	19	8094.91
5	10.68	10	114.01	15	1217.39	20	12998.93

table 2.

§5. The maximum of $\frac{\lambda(n)}{\log_2 n}$

Theorem. For every natural number $n \neq 71$,

$$\frac{\lambda(n)}{\log_2 n} < \frac{\lambda(71)}{\log_2 71}.$$

Proof. Throughout the proof we will say that $\lambda(n) \leq m$ is permitted for a natural number n in case $n > (71)^{\frac{m}{9}}$: e.g. from table 2 we see that $\lambda(n) \leq 10$ is permitted for $n \geq 115$.

Using tables 1 and 2, it is clear that if $n < 71$, then $n > (71)^{\frac{\lambda(n)}{9}}$, and hence $\frac{\lambda(n)}{\log_2 n} < \frac{\lambda(71)}{\log_2 71}$ for all $n > 71$.

Suppose now that $\lfloor \log_2 n \rfloor^+ = 7$, i.e., the binary representation of n consists of seven digits. It follows that $64 < n \leq 128$. For $72 \leq n \leq 111$, an application of (3.2) yields $\lambda(n) \leq 9$. From table 2 we see that $\lambda(n) \leq 9$

is permitted for all $n > 71$ so that $\frac{\lambda(n)}{\log_2 n} < \frac{\lambda(71)}{\log_2 71}$ for all n such that $72 \leq n \leq 111$. If $112 \leq n \leq 119$, we apply (3.4) to obtain $\lambda(n) \leq 9$ and hence it is permitted. If $120 \leq n \leq 128$, we apply (3.3) to find $\lambda(n) \leq 10$. Table 2 implies that $\lambda(n) \leq 10$ is permitted for all $n > 114$ so that we have proved the validity of $\frac{\lambda(n)}{\log_2 n} < \frac{\lambda(71)}{\log_2 71}$ for all n such that $64 < n < 128$.

If $\lceil \log_2 n \rceil^+ = 8$, then $128 < n \leq 256$. As in the preceding paragraph, applications of (3.2), (3.3), (3.4), and (3.5) yield $\lambda(n) \leq 11$. This is permitted for all $n > 183$ and so a special proof is necessary for all primes between 128 and 183. The construction of an addition chain of length less than 11 for each such prime is given in table 3 at the end of this section.

If $\lceil \log_2 n \rceil^+ = 9$, then $256 < n \leq 512$ and (3.4) and (3.5) imply that for every such n, $\lambda(n) \leq 12$. This is permitted for $n \geq 294$ and so addition chains which take less than 12 steps are given in table 3 for all primes between 256 and 294.

If $\lceil \log_2 n \rceil^+ = 10$ (i.e. $512 < n \leq 1024$), then we can apply (3.4) for $512 < n \leq 703$ to find $\lambda(n) \leq 13$. This is permitted for all $n \geq 473$. From (3.4) and (3.5) we see that for $703 < n \leq 1024$, $\lambda(n) \leq 14$. This is permitted for $n \geq 759$. Hence special chains must be constructed for all primes between 703 and 758 and this is done in table 3.

If $\lceil \log_2 n \rceil^+ = 11$ (i.e. $1024 < n \leq 2048$), then (3.4) and (3.5) assert that every such number has a chain which has length at most 15. This is permitted for $n > 1217$. Chains for the primes between 1024 and 1217 appear in table 3.

If $\lceil \log_2 n \rceil^+ = 12$ (i.e. $2048 < n \leq 4096$), then (3.4) and (3.5) imply that $\lambda(n) \leq 16$, which is permitted for all $n \geq 1955$.

If $\lceil \log_2 n \rceil^+ = 13$ (i.e. $4096 < n \leq 8192$), then (3.4) implies that for n less than 5632 there is an addition chain of length at most 17. This is permitted for all $n > 3139$. If $n \geq 5632$, a chain can be constructed of length at most 18 and this is permitted for $n > 5041$.

If $\lceil \log_2 n \rceil^+ = 14$ (i.e. if $8192 < n \leq 16384$), then (3.4) and (3.5) imply that $\lambda(n) \leq 19$, which is permitted for $n > 8094$.

Using the fact that $(71)^{\frac{4}{9}} < 2^3$ and $(71)^{\frac{16}{9}} < 2^{11}$, it follows that for

every natural number m,

$$2^{11+3m} > (71)^{\frac{16+4m}{9}}.$$

Thus, if m is a natural numer and $\lceil \log_2 n \rceil^+ = 12 + 3m$, then the above inequality and (3.4) and (3.5) imply that $\frac{\lambda(n)}{\log_2 n} < \frac{\lambda(71)}{\log_2 71}$. Similar techniques can be used to prove $\frac{\lambda(n)}{\log_2 n} < \frac{\lambda(71)}{\log_2 71}$ in case $\lceil \log_2 n \rceil^+ = 13 + 3m$ or $\lceil \log_2 n \rceil^+ = 14 + 3m$.

The proof will be completed by forming addition chains for those primes which were mentioned above. It is not known if the chains in this table are minimal, but they are sufficiently small for our purposes.

n	0	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	$\lambda(C_n)$
131	1	2	3	4	8	16	32	64	128	131						9
137	1	2	3	5	10	15	30	45	90	135	137					10
139	1	2	4	5	10	15	30	45	90	135	139					10
149	1	2	4	5	9	18	36	72	144	149						9
151	1	2	3	5	10	15	25	50	75	150	151					10
157	1	2	4	5	9	13	18	36	72	144	157					10
163	1	2	3	5	10	20	40	80	160	163						9
167	1	2	3	5	7	10	20	40	80	160	167					10
179	1	2	3	4	8	11	22	44	88	176	179					10
181	1	2	3	5	10	15	30	45	90	180	181					10
257	1	2	4	8	16	32	64	128	256	257						9
263	1	2	3	5	7	8	16	32	64	128	256	263				11
269	1	2	3	6	7	13	16	32	64	128	256	269				11
271	1	2	3	5	10	15	30	60	90	180	270	271				11
277	1	2	4	5	8	16	17	34	68	136	272	277				11
281	1	2	3	5	7	14	28	35	70	140	280	281				11
283	1	2	3	5	7	14	28	35	70	140	280	283				11
293	1	2	4	5	9	18	36	72	144	288	293					10

n	0	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	$\lambda(C_n)$
709	1	2	3	5	6	11	22	44	88	176	352	704	709			12
719	1	2	3	5	7	14	28	56	112	119	238	357	714	719		13
727	1	2	3	5	7	10	20	40	80	90	180	360	720	727		13
733	1	2	3	5	10	13	20	40	80	90	180	360	720	733		13
739	1	2	3	5	10	20	23	46	92	184	368	736	739			12
743	1	2	3	6	9	18	36	37	74	111	185	370	740	743		13
751	1	2	3	5	10	20	30	50	100	200	250	500	750	751		13
757	1	2	3	6	9	18	27	54	81	135	189	378	756	757		13
1031	1	2	3	5	7	8	16	32	64	128	256	512	1024	1031		13
1033	1	2	4	8	9	16	32	64	128	256	512	1024	1033			12
1039	1	2	3	5	10	15	16	32	64	128	256	512	1024	1039		13
1049	1	2	3	4	8	16	32	64	128	131	262	524	1048	1049		13
1051	1	2	3	4	8	16	32	64	128	131	262	524	1048	1051		13
1061	1	2	3	5	6	11	22	44	88	132	264	528	1056	1061		13
1063	1	2	3	4	7	11	22	44	66	132	264	528	1056	1063		13
1069	1	2	4	5	9	13	22	44	66	132	264	528	1056	1069		13
1087	1	2	3	5	7	9	18	27	54	81	135	270	540	1080	1087	14
1091	1	2	3	4	8	16	32	64	128	256	512	1024	1088	1091		13
1093	1	2	4	5	8	16	32	64	128	256	512	1024	1088	1093		13
1097	1	2	4	8	9	16	32	64	128	256	512	1024	1088	1097		13
1103	1	2	3	5	10	15	17	34	68	136	272	544	1088	1103		13
1109	1	2	4	8	16	17	21	34	68	136	272	544	1088	1109		13
1117	1	2	4	8	9	18	36	72	108	180	360	540	1080	1116	1117	14
1123	1	2	3	5	7	14	28	35	70	140	280	560	1120	1123		13
1129	1	2	4	5	6	9	15	30	35	70	140	280	560	1120	1129	14
1151	1	2	4	8	16	17	21	42	63	126	189	378	756	1134	1151	14
1153	1	2	4	8	16	32	64	128	256	512	1024	1152	1153			12
1163	1	2	3	5	6	11	16	32	64	128	256	512	1024	1152	1163	14
1171	1	2	3	6	9	18	36	72	73	146	292	584	1168	1171		13
1181	1	2	3	5	7	14	21	35	49	98	147	294	588	1176	1181	14
1187	1	2	3	6	9	18	36	37	74	148	296	592	1184	1187		13
1193	1	2	3	6	9	18	36	37	74	148	296	592	1184	1193		13
1201	1	2	3	5	10	15	30	60	75	150	300	600	1200	1201		13
1213	1	2	3	5	10	13	15	30	60	75	150	300	600	1200	1213	14
1217	1	2	3	5	10	15	17	30	60	75	150	300	600	1200	1217	14

table 3

This table completes the proof of the theorem

Appendix

We only comment on the entries in table 1 for $n \leq 71$.

1. We recall first that every addition chain is ordered by the relation $<$.

2. An obvious inequality is

$$\lambda(n) \geq \min\{(\max\{\lambda(p), \lambda(q)\} | p+q = n\} + 1.$$

In case equality occurs for some n, no comment is made about that entry for n in the table.

3. If $\min\{\max\{\lambda(p), \lambda(q)\} | p+q = n\} = \lambda(p_0) = \lambda(q_0)$ and if $p \neq q$, then it is easy to see that we cannot have an addition chain for n in $\lambda(p_0) + 1$ steps in which both p and q occur. In case this occurs, no further remark will be made about it.

4. It is obvious that 2^m can be constructed only along powers of 2 in m steps. Moreover, 3.2^m can be constructed only along powers of 2 and 3 times a power of 2 in m+2 steps. If n is the sum of 2^m or 3.2^m and another number, no comment is necessary if n cannot be made in m+1 or m+3 steps.

5. In commenting on the remaining numbers, we denote the possible place of a number in a chain with a Roman numeral. The remaining comments concern the elimination of a number m in making a chain for a number n; i.e. m cannot be at a certain place in a minimal chain for n in case some other thing must occur.

For n = 11: If 8 is at III, then 3 cannot be at II.
For n = 19: If 16 is at IV, then 3 cannot be at II.
For n = 21: If 16 is at IV, then 5 cannot be at III.
For n = 29: If 20 is at V, then 9 cannot be at IV.
Since 17 cannot be made in 5 steps along 12 and
if 12 is at IV, then 17 cannot be at V.
For n = 31: If 24 is at V, then 7 is not in the chain.
If 15 is at V, then 16 is at least at VI.
For n = 47: If 7 is at IV, then 40 cannot be at VI.
If 11 is at V, then 36 cannot be at VI.
If 13 is at V, then 34 cannot be at VI.

If 14 is at V, then 33 cannot be at VI.

If 15 is at V, then 32 cannot be even at VI.

If 17 is at V, then 30 cannot be at VI.

If 20 is at V, then 27 cannot be at VI.

For n = 53: If 13 is at V, then 40 cannot be at VI.

If 17 is at V, then 36 cannot be at VI.

If 20 is at V, then 33 cannot be at VI.

For n = 55: If 40 is at VI, then 15 cannot be at V.

For n = 57: If 40 is at VI, then 17 cannot be at V.

If 24 is at V then 33 cannot be at VI.

For n = 58: If 40 is at VI, then 18 cannot be at V.

If 24 is at V, then 34 cannot be at VI.

For n = 71: If 68 is at VII, then 8 must be at III and 3 cannot be at II.

If 66 is at VII, then 16 must be at IV and 5 cannot be at III.

If 65 is at VII, then 32 must be at V and 6 cannot be at III.

If 7 is at VI, then 64 cannot even be at VII.

If 11 is at V, then 60 cannot be at VII.

If 15 is at V, then 56 cannot be at VII.

If 17 is at V, then 54 cannot be at VII.

If 19 is at VI, then 52 cannot be at VII.

If 20 is at V, then there is an even number at IV,
and we have to add an odd number in order to get 51.
Therefore 51 cannot be at VII.

If 21 is at VI, then 50 cannot be at VII.

If 22 is at VI, then 49 cannot be at VII.

If 23 is at VI, then 48 cannot even be at VII.

If 25 is at VI, then 21 and 23 cannot be at VI, and
hence 46 cannot be at VII.

If 26 is at VI, then 19 cannot be at VI, and hence 45 cannot
be at VII.

If 27 is at VI, then 17 cannot be at V, and hence 44 cannot
be at VII.

If 28 is at VI, then 15 cannot be at V, and hence 43 cannot
be at VII.

If 30 is at VI, then 11 cannot be at V, and hence 41 cannot
be at VII.

If 39 is at VII, then 32 cannot be at V or VI.

If 33 is at VI, then 38 cannot be at VII.

If 34 is at VI, then 37 cannot be at VII.

These remarks together indicate that the entries in table 1 are correct for $n \leq 71$.

References.

[1] R. Bellman, Problem 5152 Am. Math. Monthly, 70 (1963) 765.

[2] A. Brauer, On addition chains, Bull. Am. Math. Soc. 45 (1939) 736-739.

[3] A. Scholz, Jahresbericht der Deutschen Math. Ver. 47-2 (1937) 41-42.

[4] E.G. Strauss, Addition chains of vectors, Am. Math. Monthly 71 (1964) 807-808.

Addendum

It might seem from the report that we have ignored some problems concerning $\lambda(n)$ since we have only discussed upper bounds for $\lambda(n)$. In fact, the actual computation of $\lambda(n)$ appears to be very difficult and even trying to find a non-trivial lower bound for $\lambda(n)$ seems to be as difficult as trying to compute $\lambda(n)$. In any case, we wish to include a few conjectures and a brief discussion of them.

We have seen from section 2 that

(1) $\lambda(n) \leq \lambda(r) + \lambda(s)$ for $n = rs$,

(2) $\lambda(p) \leq \lambda(p-1) + 1$ for p is a prime.

We define a new function θ by

$$\theta(1) = 0,$$
$$\theta(n) = \theta(r) + \theta(s) \quad \text{for } n = rs,$$
$$\theta(p) = \theta(p-1) + 1 \quad \text{for } p \text{ is a prime.}$$

It was conjectured that a study of this function θ would help in the study of λ. We will show that the behavior of θ is different from the behavior of λ by showing $\limsup_{n\to\infty} \frac{\theta(n) - \lambda(n)}{\log_2 n} > 0$.

Proof. Let $n = 23$. We know that $\lambda(23) = 6$ and it is easily seen that $\theta(23) = 7$. Moreover, if n and k are natural numbers, then $\theta(n) \geq \lambda(n)$, $\lambda(n^k) \leq k\lambda(n)$, and $\theta(n^k) = k\theta(n)$. Therefore,

$$\limsup_{n\to\infty} \frac{\theta(n) - \lambda(n)}{\log_2 n} \geq \limsup_{k\to\infty} \frac{\theta(23^k) - \lambda(23^k)}{\log_2 23^k}$$

$$\geq \limsup_{k\to\infty} \frac{k\theta(23) - k\lambda(23)}{k \log_2 23} = \frac{\theta(23) - \lambda(23)}{\log_2 23} \geq \frac{1}{5} > 0.$$

It follows that θ does not help.

From table 1, one might conjecture that

(3) $\lambda(2n+1) \geq \lambda(2n)$ for all n.

However, one can show that $\lambda(255) \leq 10$ and $\lambda(254) = 11$.
In fact, $\lambda(255) \leq 10$ follows from (1) and $\lambda(254) = 11$ can be shown by

a technique similar to that which appeared in the appendix.

Also from table 1, it appears that

(4) $\lambda(2n) = \lambda(n) + 1$ for all n.

Indeed, if for example n is of the form $q.2^m$ for q = 1, 3, 5, 7, 9, 11, then (4) holds. Nevertheless, for the number 2n whose binary representation is

10101010101010101010101010110,

we have constructed an addition chain which takes 35 steps, but we have not succeeded in constructing a chain for n with length less than 35.

Another conjecture was that for each n there exists a minimal chain $n_0, \ldots, n_k$ such that one can always use n_j to construct n_{j+1}; e.g. $n_{j+1} = n_j + n_j$ or $n_{j+1} = n_j + n_s$, $s < j$. There exist counter-examples to this conjecture, but the numbers involved are rather large.