Minimizing sums of addition chains

H. Zantema

RUU-CS-89-15
June 1989

Rijksuniversiteit Utrecht

Vakgroep informatica

Padualaan 14 3584 CH Utrecht
Corr. adres: Postbus 80.089, 3508 TB Utrecht
Telefoon 030-531454
The Netherlands

Minimizing sums of addition chains

H. Zantema

RUU-CS-89-15
June 1989

Rijksuniversiteit Utrecht

Vakgroep informatica

Padualaan 14 3584 CH Utrecht
Corr. adres: Postbus 80.089, 3508 TB Utrecht
Telefoon 030-531454
The Netherlands

Minimizing sums of addition chains

H. Zantema

Technical Report RUU-CS-89-15
June 1989

Department of Computer Science
University of Utrecht
P.O.Box 80.089, 3508 TB Utrecht
The Netherlands

Minimizing sums of addition chains

H. Zantema
Department of Computer Science
University of Utrecht
P.O. box 80.089
3508 TB Utrecht
The Netherlands

Abstract

The length of an addition chain for n measures the number of multiplications for computing x^n from x. If the cost of the multiplications is taken into account, then the *sum* of the elements of an addition chain for n is a better measure for the cost of computing x^n than the length.

In this paper bounds on sums of addition chains are derived, and properties of optimal addition chains according to the sum cost criterion are studied. It turns out that the last step in an optimal addition chain for an even number is always a doubling, and the sum of an optimal addition chain for an odd number n is asymptotically very close to $5n/2$.

1 Introduction

1.1 Motivation

In [1], section 4.6.3, an extensive study of lengths of addition chains is given. An *addition chain for* n is defined to be a sequence of integers

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = n$$

with the property that for all $i = 1, 2, \ldots r$ there exist k and j with $k \leq j < i$ and

$$a_i = a_j + a_k.$$

The motivation for studying addition chains is the following:

> If there exists an addition chain of length r for n, then x^n can be computed in r multiplications from x.

In this motivation, however, only the *number* of multiplications is counted. It is reasonable to take into account that a multiplication of large numbers is more expensive than a multiplication of small numbers. If the classical multiplication algorithm is used then the cost of a multiplication is approximated by the product of the numbers of bits of the multiplicands. Building $a_i = a_j + a_k$ from a_j and a_k then gives a cost $a_j * a_k$. In [2] it has been shown that for this cost function on addition chains, the addition chain for n obtained by steps of adding one and doubling according to the binary representation of n, is optimal.

However, there are faster multiplication algorithms. The cost of a multiplication of two integers by the Schönhage–Strassen algorithm is proportional to

$$p \log p \log \log p$$

where p is the number of digits of the result, see e.g. [3], section 7.5. If the logarithmic factors are ignored, so the cost of multiplication is postulated to be proportional to the length p of the result, then building $a_i = a_j + a_k$ from a_j and a_k requires a cost proportional to a_i. Note that the cost of merely writing down the result of a multiplication as a p-bit number is also proportional to p.

In this approach the total cost of computing x^n using an addition chain for n is proportional to the sum of the elements of the addition chain. In this paper we derive bounds on sums of addition chains, and study properties of optimal addition chains according to this sum cost criterion.

1.2 Definition and summary of results

First we give a definition.

Definition 1 *For a positive integer n the* optimal chain sum $S(n)$ *is the smallest value such that*

$$S(n) = \sum_{i=1}^{r} a_i$$

for an addition chain

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = n.$$

Any addition chain for n that achieves a sum of $S(n)$ is called optimal. *For $n > 1$ the* ratio $\rho(n)$ *of n is defined to be $S(n)/(n-1)$. For consistency we define $\rho(1) = 5/2$.*

If $a_k < a_{k-1}$ in any addition chain, then the chain in which a_k and a_{k-1} are interchanged is also an addition chain. Thus we may restrict ourselves to increasing addition chains without any loss of generality. If an element occurs more than once in an addition chain, then the chain remains an addition chain after removing a copy. So throughout this paper we may, and shall, assume without any loss of generality that all addition chains are strictly increasing.

We shall prove that

$$\rho(n) \geq \frac{5}{2}$$

for all odd n, while equality holds if and only if n is a power of 2 plus one, or a product of numbers of that shape.

On the other hand we shall prove that

$$\rho(n) \leq \frac{5}{2} + O(n^{-1/2}),$$

for all positive integers n.

For even n let m be the greatest odd divisor of n. We shall prove that any optimal addition chain for n is obtained by extending an optimal addition chain for m by the chain

$$2m,\ 4m,\ \ldots,\ 2^{\cdots}m = n.$$

Hence optimal addition chains for even numbers are immediately derived from optimal addition chains for odd numbers and we may focus on odd numbers. The optimal addition chains for all odd numbers less than 60 are listed in table 1.

As we might expect, the last element of an optimal addition chain for an odd number is always the sum of the two elements preceding it. In section 5 we prove that this holds in general. Furthermore we show that the one but last element of an optimal addition chain for an odd number not divisible by 3, is always odd, except in the case of a few small numbers.

Many of the proofs in this paper are given in the following way. Assume that an optimal addition chain for n does not have the shape that is claimed. Lower bounds

n	$S(n)$	$\rho(n)$	chain(s)	n	$S(n)$	$\rho(n)$	chain(s)
1	0	2.5000	1	31	78	2.6000	1, 2, 3, 4, 7, 14, 17, 31
3	5	2.5000	1, 2, 3	33	80	2.5000	1, 2, 4, 8, 16, 17, 33
5	10	2.5000	1, 2, 3, 5	35	86	2.5294	1, 2, 3, 4, 7, 14, 21, 35
7	16	2.6667	1, 2, 3, 4, 7	37	92	2.5556	1, 2, 3, 5, 8, 16, 21, 37
9	20	2.5000	1, 2, 4, 5, 9	39	96	2.5263	1, 2, 3, 6, 7, 13, 26, 39
			1, 2, 3, 6, 9				1, 2, 3, 5, 8, 13, 26, 39
11	27	2.7000	1, 2, 3, 5, 6, 11	41	102	2.5500	1, 2, 4, 5, 9, 18, 23, 41
			1, 2, 3, 4, 7, 11				1, 2, 3, 5, 10, 20, 21, 41
13	31	2.5833	1, 2, 3, 6, 7, 13	43	106	2.5238	1, 2, 3, 5, 10, 20, 23, 43
			1, 2, 3, 5, 8, 13	45	110	2.5000	1, 2, 4, 5, 9, 18, 27, 45
15	35	2.5000	1, 2, 3, 6, 9, 15				1, 2, 3, 6, 9, 18, 27, 45
			1, 2, 3, 5, 10, 15				1, 2, 3, 6, 9, 15, 30, 45
17	40	2.5000	1, 2, 4, 8, 9, 17				1, 2, 3, 5, 10, 20, 25, 45
19	47	2.6111	1, 2, 3, 4, 8, 11, 19				1, 2, 3, 5, 10, 15, 30, 45
21	51	2.5500	1, 2, 3, 4, 7, 14, 21	47	120	2.6087	1, 2, 3, 4, 7, 10, 20, 27, 47
23	56	2.5455	1, 2, 3, 5, 10, 13, 23	49	121	2.5208	1, 2, 3, 6, 12, 24, 25, 49
25	60	2.5000	1, 2, 3, 5, 10, 15, 25	51	125	2.5000	1, 2, 4, 8, 9, 17, 34, 51
27	65	2.5000	1, 2, 4, 5, 9, 18, 27				1, 2, 3, 6, 12, 24, 27, 51
			1, 2, 3, 6, 12, 15, 27	53	134	2.5769	1, 2, 3, 5, 6, 12, 24, 29, 53
			1, 2, 3, 6, 9, 18, 27	55	137	2.5370	1, 2, 3, 5, 6, 11, 22, 33, 55
29	74	2.6429	1, 2, 3, 5, 6, 12, 17, 29				1, 2, 3, 4, 7, 11, 22, 33, 55
			1, 2, 3, 4, 7, 14, 15, 29	57	142	2.5357	1, 2, 3, 4, 8, 11, 19, 38, 57
			1, 2, 3, 4, 7, 11, 18, 29	59	148	2.5517	1, 2, 3, 4, 7, 14, 28, 31, 59

Table 1: Optimal addition chains for the odd integers < 60.

on $\rho(m)$ for various elements m occurring in the tail part of this optimal addition chain for n give some inequalities. Then a linear combination of these inequalities is found giving a lower bound on $\rho(n)$, conflicting the upper bound on $\rho(n)$ for n large enough. Some case analysis is often inevitable. For small n the proof is given by direct verification.

In the last two sections some remarks and open problems are given concerning star chains and the lengths of optimal addition chains. It turns out that all our bounds and results on the shape of optimal addition chains also hold for optimal star chains, except for the explicit constant we can reach in the O of the result

$$\rho(n) \leq \frac{5}{2} + O(n^{-1/2}).$$

2 Lower bounds on optimal chain sums

Lemma 1 *Let*

$$\ldots, a_k, \ldots, a_r$$

be any addition chain. Then

$$\sum_{i=k+1}^{r} a_i \geq 2(a_r - a_k).$$

Equality only holds for the chain

$$\ldots, a_k, 2a_k, \ldots, 2^{r-k}a_k = a_r$$

Proof: By induction to $r - k$. For $r = k$ it is trivial. For $r > k$ we have

$$\sum_{i=k+1}^{r} a_i = \sum_{i=k+1}^{r-1} a_i + a_r \geq 2(a_{r-1} - a_k) + a_r \geq 2(a_r - a_k)$$

since $a_r \leq 2a_{r-1}$ by the definition of an addition chain.

The second assertion follows the same induction: if anywhere $a_r < 2a_{r-1}$ then a strict inequality appears. □

This lemma is one of the basic tools for deriving bounds on $\rho(n)$; we shall often refer to it without explicitly mentioning it.

An immediate consequence by choosing $k = 0$ is the following:

Proposition 1 *For all positive integers n we have*

$$\rho(n) \geq 2,$$

where equality holds if and only if n is a power of 2.

Proposition 2 *For all positive odd integers n we have*

$$\rho(n) \geq \frac{5}{2},$$

where equality holds if and only if $n = 1, 3, 5, 9, 15, 17, 25, 27, 33, \ldots$, i.e. n can be written as

$$\prod_i (2^{\nu(i)} + 1).$$

Proof: We shall prove that

$$S(n) \geq \frac{5}{2}(n-1)$$

for n odd by induction to n. For $n = 1$ this holds. For $n > 1$ let

$$1 = a_0,\ a_1,\ a_2,\ \ldots,\ a_r = n$$

be an optimal addition chain for n. By definition of an addition chain we have

$$n = a_r = a_s + a_t$$

for some $s, t < r$. Since n is odd we have $s \neq t$; we may assume

$$s < t < r.$$

We distinguish three cases:

1. a_t is even;
2. a_t is odd and $s \neq t-1$;
3. a_t is odd and $s = t-1$.

case 1: a_t is even.
From the induction hypothesis and a_s is odd we conclude that

$$\sum_{i=1}^{s} a_i \ \geq \ \frac{5}{2}(a_s - 1).$$

Since $\sum_{i=s+1}^{t} a_i \geq a_t$ and $\sum_{i=s+1}^{t} a_i \geq 2(a_t - a_s)$ we also have

$$\sum_{i=s+1}^{t} a_i \ \geq \ \frac{a_t}{2} + (a_t - a_s) \ = \ \frac{3n - 5a_s}{2}.$$

Further we have

$$\sum_{i=t+1}^{r} a_i \ \geq \ a_r \ = \ n.$$

We conclude that

$$S(n) = \sum_{i=1}^{r} a_i \geq \frac{5}{2}(a_s - 1) + \frac{3n - 5a_s}{2} + n = \frac{5}{2}(n-1),$$

which we had to prove.

case 2: a_t is odd and $s \neq t-1$.

We have

$$\sum_{i=1}^{s} a_i \geq 2(a_s - 1).$$

Since $s < t-1$ we have $\sum_{i=s+1}^{t} a_i > a_s + a_t$. We also have $\sum_{i=s+1}^{t} a_i \geq 2(a_t - a_s)$, so we obtain

$$\sum_{i=s+1}^{t} a_i > \frac{a_s + a_t}{2} + (a_t - a_s) = \frac{3n - 4a_s}{2}.$$

Again we have

$$\sum_{i=t+1}^{r} a_i \geq a_r = n.$$

We conclude that

$$S(n) = \sum_{i=1}^{r} a_i > 2(a_s - 1) + \frac{3n - 4a_s}{2} + n > \frac{5}{2}(n-1),$$

which we had to prove. Note the strict inequality: if $\rho(n) = \frac{5}{2}$ then this case 2 will never occur.

case 3: a_t is odd and $s = t-1$.

There must be u and v such that $a_t = a_u + a_v$. Since a_t is odd either a_u or a_v is odd, say a_u. From the induction hypothesis we conclude that

$$\sum_{i=1}^{u} a_i \geq \frac{5}{2}(a_u - 1).$$

Further we have

$$\sum_{i=u+1}^{s} a_i \geq 2(a_s - a_u)$$

and

$$\sum_{i=s+1}^{r} a_i \geq a_t + n.$$

From $s = t-1$ we obtain $a_s \geq a_v$, and we conclude that

$$\begin{aligned} S(n) = \sum_{i=1}^{r} a_i &\geq \frac{5}{2}(a_u - 1) + 2(a_s - a_u) + a_t + n \\ &= \frac{1}{2}a_u + 2a_s + a_t + n - \frac{5}{2} \\ &\geq \frac{1}{2}a_u + \frac{1}{2}a_v + \frac{3}{2}a_s + a_t + n - \frac{5}{2} \\ &= \frac{5}{2}(n-1), \end{aligned}$$

which we had to prove.

It remains to show that, if n is odd, then $\rho(n) = \frac{5}{2}$ holds if and only if n is a product of numbers of the shape $2^k + 1$. Then in the above case distinction all inequalities have to be sharp. This is only possible in cases 1 and 3.

In case 1 two of the inequalities were

$$\sum_{i=s+1}^{t} a_i \geq a_t \text{ and } \sum_{i=s+1}^{t} a_i \geq 2(a_t - a_s).$$

If both inequalities are sharp then $a_t = 2(a_t - a_s)$, so $a_t = 2a_s$, and

$$n = a_s + a_t = 3a_s.$$

In case 3 we applied the inequality

$$\sum_{i=u+1}^{s} a_i \geq 2(a_s - a_u),$$

which is sharp only if $a_s = 2^k a_u$ for some positive integer k. We also applied the inequality $a_s \geq a_v$, which is sharp only if $a_s = a_v$. Then we have

$$n = a_s + a_t = 2a_s + a_u = (2^{k+1} + 1)a_u.$$

We have proved by induction that the only candidates for equality are products of numbers of the shape $2^k + 1$.

On the other hand, for all of these numbers an addition chain giving $\rho(n) = \frac{5}{2}$ can be constructed: if

$$1 = a_0, a_1, a_2, \ldots, a_r = n$$

is a chain giving $\rho(n) = \frac{5}{2}$, then

$$1 = a_0, a_1, a_2, \ldots, a_r = n, 2n, \ldots, 2^{k-1}n, (2^{k-1} + 1)n, (2^k + 1)n$$

is a chain giving $\rho((2^k + 1)n) = \frac{5}{2}$. □

The optimal addition chain for a product of numbers of the shape $2^k + 1$ is unique up to the chosen order of the factors of the product. This is forced by the proof of the above proposition. For example, if 15 is considered as $3 * 5$, then we obtain the optimal addition chain

$$1, 2, 3, 6, 9, 15.$$

On the other hand, if 15 is considered as $5 * 3$, then we obtain the optimal addition chain

$$1, 2, 3, 5, 10, 15.$$

For 9 we obtain the two optimal addition chains

$$1, 2, 3, 6, 9 \text{ and } 1, 2, 4, 5, 9$$

by considering 9 as $3*3$ and as 2^3+1 respectively. The five optimal addition chains for 45 in table 1 are obtained by considering 45 respectively as $(2^3+1)*5, 3*3*5, 3*5*3, 5*(2^3+1)$ and $5*3*3$.

Until now we focussed on lower bounds on $\rho(n)$ for odd n. In section 4 we shall prove that $S(2n) = S(n) + 2n$ for all positive integers n, and as a consequence for $n = 2^k * m$, m odd:

$$\rho(n) \geq 2 + \frac{m-1}{2(n-1)}$$

where equality holds if and only if m is a (possibly empty) product of powers of 2 plus one.

Before we can derive this lower bound, we first need upper bounds on $\rho(n)$.

3 Upper bounds on optimal chain sums

In this section we sometimes need bounds on the sum of an addition chain containing more than one fixed element. That's why we start with a definition.

Definition 2 *For a sequence of non-negative integers $b_1, \ldots, b_s$ the value $S(b_1, \ldots, b_s)$ is the smallest value such that*

$$S(b_1, \ldots, b_s) = \sum_{i=1}^{r} a_i$$

for an addition chain

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r$$

for which

$$(\forall i : 1 \leq i \leq s : b_i = 0 \vee (\exists j : 0 \leq j \leq r : a_j = b_i)).$$

The corresponding chain is called optimal *for $b_1, \ldots, b_s$.*

The key lemma for deriving upper bounds is the following.

Lemma 2 *Let $n = m*2^k + a$ for $k \geq 1, m > 0, a \geq 0$, and let $b_1, \ldots, b_s$ be a possibly empty sequence of non-negative integers. Then*

$$S(n, b_1, \ldots, b_s) \leq \frac{5n}{2} + S(m, b_1, \ldots, b_s, a) - \frac{a}{2} - 2m.$$

Proof: Let

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r$$

be an optimal addition chain for $m, b_1, \ldots, b_s, a$. Then

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r,\ 2m, \ldots,\ 2^{k-1}m,\ 2^{k-1}m + a,\ 2^k m + a = n$$

is an addition chain for $n, b_1, \ldots, b_s$. We obtain

$$\begin{aligned} S(n, b_1, \ldots, b_s) &\leq S(m, b_1, \ldots, b_s, a) + (2^k - 2)m + 2^{k-1}m + a + 2^k m + a \\ &= \frac{5}{2}(2^k m + a) + S(m, b_1, \ldots, b_s, a) - \frac{a}{2} - 2m \\ &= \frac{5n}{2} + S(m, b_1, \ldots, b_s, a) - \frac{a}{2} - 2m. \end{aligned}$$

□

The following proposition gives a general applicable upper bound on $S(n)$; it will be used as a basic tool in most of the propositions that follow.

Proposition 3 *For all positive integers n we have*

$$S(n) < \frac{18n}{7}.$$

Proof: For $n < 8$ the proposition is easily verified. For $n \geq 8$ we shall prove the following more general property:

> **Property** For each integer $n \geq 8$ and for each possibly empty sequence $b_1, \ldots, b_s$ of positive odd numbers, all < 8, we have
>
> $$S(n, b_1, \ldots, b_s) < \frac{18n + 4\sum_{i=1}^{s} b_i}{7}.$$

We shall prove this property by induction to n using lemma 2 for $k = 3$.

It has been verified by a computer program that for every n with $8 \leq n < 64$:

- there is an addition chain starting with $1, 2, 3$ for which the sum is less than $18n/7$;
- there is an addition chain starting with $1, 2, 3, 5$ for which the sum is less than $(18n + 20)/7$;
- there is an addition chain starting with $1, 2, 3, 4, 7$ or $1, 2, 3, 5, 7$ or $1, 2, 3, 6, 7$ for which the sum is less than $(18n + 28)/7$;
- there is an addition chain starting with $1, 2, 3, 5, 7$ or $1, 2, 3, 4, 5, 7$ for which the sum is less than $(18n + 48)/7$.

We conclude that the property holds for $n < 64$.

For $n \geq 64$ write $n = 8m + a$ with $m \geq 8$ and $0 \leq a < 8$. By definition we have

$$S(m, b_1, \ldots, b_s, 0) = S(m, b_1, \ldots, b_s);$$

since 2 is contained in every non-trivial addition chain we have

$$S(m, b_1, \ldots, b_s, 2) = S(m, b_1, \ldots, b_s).$$

Combining this by the induction hypothesis we obtain

$$S(m, b_1, \ldots, b_s, a) < \frac{18m + 4a + 4\sum_{i=1}^{s} b_i}{7} \tag{1}$$

for $a \neq 4, 6$.

Let $a \neq 4, 6$. Applying lemma 2 for $k = 3$ and 1 we obtain

$$\begin{aligned} S(n, b_1, \ldots, b_s) &\leq \frac{5n}{2} + S(m, b_1, \ldots, b_s, a) - \frac{a}{2} - 2m \\ &< \frac{5n}{2} + \frac{18m + 4a + 4\sum_{i=1}^{s} b_i}{7} - \frac{a}{2} - 2m \\ &= \frac{5n}{2} + \frac{8m + a}{14} + \frac{4\sum_{i=1}^{s} b_i}{7} \\ &= \frac{18n + 4\sum_{i=1}^{s} b_i}{7}. \end{aligned}$$

It remains to prove the property for $n = 8m + a$ with $m \geq 8$ and $a = 4$ or $a = 6$. Let α be an optimal addition chain for $m, b_1, \ldots, b_s,\ a/2$. Then

$$\alpha,\ 2m,\ 2m + \frac{a}{2},\ 4m + \frac{a}{2},\ 8m + a = n$$

is an addition chain containing $n, b_1, \ldots, b_s$. Hence

$$S(n, b_1, \ldots, b_s) \leq S(m, b_1, \ldots, b_s, \frac{a}{2}) + 16m + 2a = S(m, b_1, \ldots, b_s, \frac{a}{2}) + 2n.$$

Applying 1 for a replaced by $a/2$ we obtain

$$\begin{aligned} S(n, b_1, \ldots, b_s) &\leq S(m, b_1, \ldots, b_s, \frac{a}{2}) + 2n \\ &< \frac{18m + 2a + 4\sum_{i=1}^{s} b_i}{7} + 2n \\ &< \frac{32m + 4a + 4\sum_{i=1}^{s} b_i}{7} + 2n \\ &= \frac{18n + 4\sum_{i=1}^{s} b_i}{7}. \end{aligned}$$

This concludes the proof of the property, and hence of the proposition. □

This bound is rather sharp; for example

$$\frac{S(71)}{71} = \frac{182}{71} \approx 2.5634 < 2.5714 \approx \frac{18}{7}.$$

A direct consequence is the following result on $\rho(n)$.

Proposition 4 *For all positive integers n we have*

$$\rho(n) \leq \frac{27}{10},$$

where equality holds if and only if $n = 11$.

Proof: For $n < 21$ we refer to table 1. For $n \geq 21$ we obtain

$$\rho(n) = \frac{S(n)}{n-1} < \frac{18}{7} * \frac{n}{n-1} \leq \frac{18}{7} * \frac{21}{20} = \frac{27}{10}.$$

□

The bound of proposition 3 was achieved by applying lemma 2 for a fixed number $k = 3$. For large n the upper bound on $S(n)$ can be improved by taking larger values of k, as is done in the next proposition.

Proposition 5 *For all integers $n > 1$ we have*

$$S(n) < \frac{5n}{2} + c\sqrt{n},$$

where $c = \frac{3}{7}\sqrt{29} \approx 2.308$. As a consequence we have

$$\rho(n) \leq \frac{5}{2} + O(n^{-\frac{1}{2}}).$$

Proof: By elementary calculus it is easily shown that

$$\frac{29x}{14} + \frac{4n}{7x} \leq \frac{3}{7}\sqrt{29n}$$

for each value x for which

$$2\sqrt{\frac{n}{29}} \leq x \leq 4\sqrt{\frac{n}{29}}.$$

Choose the integer k such that

$$2\sqrt{\frac{n}{29}} \leq 2^k \leq 4\sqrt{\frac{n}{29}},$$

and write $n = 2^k m + a$ with $0 \leq a < 2^k$. Then by lemma 2 we obtain

$$\begin{aligned}
S(n) &\leq \frac{5n}{2} + S(m,a) - \frac{a}{2} - 2m \\
&\leq \frac{5n}{2} + S(m) + S(a) - \frac{a}{2} - 2m \\
&< \frac{5n}{2} + \frac{18m + 18a}{7} - \frac{a}{2} - 2m \\
&= \frac{5n}{2} + \frac{29a}{14} + \frac{4m}{7} \\
&< \frac{5n}{2} + \frac{29 * 2^k}{14} + \frac{4n}{7 * 2^k} \\
&\leq \frac{5n}{2} + \frac{3}{7}\sqrt{29n}.
\end{aligned}$$

□

For small numbers we shall always use the bound $18n/7$; only for $n > 1044$ the bound of proposition 5 is better than $18n/7$.

The next proposition compares addition chains for mn with addition chains for m and for n.

Proposition 6 *For all integers m and n both > 1 we have*

$$\rho(mn) \leq \frac{\rho(m) + \rho(n)}{2}.$$

Proof: By symmetry we may assume that $\rho(n) \geq \rho(m)$. Let

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = n$$

be an optimal addition chain for n and

$$1 = b_0,\ b_1,\ b_2, \ldots,\ b_s = m$$

an optimal addition chain for m. Then

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r,\ a_r b_1,\ a_r b_2, \ldots,\ a_r b_s = mn$$

is an addition chain for mn. So we have

$$\begin{aligned} S(mn) &\leq S(n) + nS(m) \\ &= (n-1)\rho(n) + n(m-1)\rho(m) \\ &\leq (n-1)\rho(n) + n(m-1)\rho(m) + (n(m-1) - (n-1))(\frac{\rho(n) - \rho(m)}{2}) \\ &= (mn-1)\frac{\rho(m) + \rho(m)}{2}, \end{aligned}$$

so

$$\rho(mn) = \frac{S(mn)}{mn-1} \leq \frac{\rho(m) + \rho(n)}{2}.$$

□

4 Optimal addition chains for even numbers

Combining proposition 1 and proposition 3 we are now able to prove that the last step in an optimal addition chain for an even number is always a doubling.

Proposition 7 *Let $n \geq 1$ and let*

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = 2n$$

be an optimal addition chain for $2n$. Then $a_{r-1} = n$ and

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_{r-1} = n$$

is an optimal addition chain for n.

Proof: Assume the assertion does not hold. Then the last step in the addition chain is not a doubling, and there exist s and t such that

$$a_s < a_t < a_r = 2n \quad \text{with} \quad a_s + a_t = 2n.$$

We have the following inequalities:

$$S(2n) \leq S(n) + 2n,$$
$$S(a_s) + a_t + 2n \leq S(2n),$$
$$S(a_t) + 2n \leq S(2n).$$

According to proposition 1 we have

$$S(a_s) \geq 2a_s - 2 \quad \text{and} \quad S(a_t) \geq 2a_t - 2.$$

According to proposition 3 we have

$$S(n) < \frac{18n}{7}.$$

Combining these results we obtain

$$2a_s - 2 + a_t < \frac{18n}{7}$$

and

$$a_t - 1 < \frac{9n}{7}.$$

Adding these inequalities gives

$$4n - 3 = 2(a_s + a_t) - 3 < \frac{27n}{7},$$

so $n < 21$. For $n < 21$ it is easily verified that the assertion holds. This contradicts our assumption. □

Note that this behaviour of optimal addition chains differs from the behaviour with respect to the length criterion of addition chains: in [1] it is mentioned that the last step of a shortest addition chain for 382 is never a doubling. This also proves that a shortest optimal addition chain for 382 is longer than a shortest addition chain for 382.

A direct consequence of the proposition is the following.

Proposition 8 *Let $n \geq 1$ and $k \geq 0$, and let*

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = 2^k n$$

be an optimal addition chain for $2^k n$. Then $a_{r-i} = 2^{k-i} n$ for $i = 0, 1, \ldots, k$ and

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_{r-k} = n$$

is an optimal addition chain for n. As a consequence

$$S(2^k n) = S(n) + (2^{k+1} - 2)n.$$

Combining this result with propositions 2 and 5 we obtain the following main result.

Proposition 9 *Let $n \geq 1$ and write $n = 2^k * m$, m odd. Then*

$$2n + \frac{m}{2} - \frac{5}{2} \leq S(n) < 2n + \frac{m}{2} + c\sqrt{m}$$

for $c = 2.308$, and

$$2 + \frac{m-1}{2(n-1)} \leq \rho(n) \leq 2 + \frac{m-1}{2(n-1)} + O(2^{-k} * m^{-\frac{1}{2}}).$$

The left inequalities are equalities if and only if m can be written as a (possibly empty) product

$$\prod_i (2^{\nu(i)} + 1).$$

5 The shape of optimal addition chains

In this section the shape of optimal addition chains is discussed, in particular we consider what can be said about the last few steps of them. As the shape of optimal addition chains for even numbers was determined in section 4, we now restrict to odd numbers. The results imply strong optimizations of backtracking algorithms for finding optimal addition chains. These optimizations have been used to check that there are no more optimal addition chains for 137 and 145 than those listed in sections 6 and 7.

Proposition 10 *Let*

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = n$$

be an optimal addition chain for an odd number $n > 1$. Then

$$n = a_{r-1} + a_{r-2}.$$

Proof: If n cannot be written as $a_{r-1} + a_s$ for some s, then the number a_{r-1} can simply be removed from the addition chain, making the sum smaller. So $n = a_{r-1}+a_s$ for some s. Since n is odd we have $s < r-1$. Assume the proposition does not hold, so $s < r-2$.

We distinguish two cases: a_s is odd and a_s is even. First assume a_s is odd. Then

$$\sum_{i=1}^{s} a_i \;\geq\; \frac{5}{2}(a_s - 1).$$

Since $\sum_{i=s+1}^{r-1} a_i \geq a_{r-2}+a_{r-1} > a_s+a_{r-1} = n$ and $\sum_{i=s+1}^{r-1} a_i \geq 2(a_{r-1}-a_s) = 2n-4a_s$ we also have

$$\sum_{i=s+1}^{r-1} a_i \;>\; \frac{3}{8}n + \frac{5}{8}(2n - 4a_s).$$

We conclude that

$$\frac{18}{7}n \;>\; S(n) \;=\; \sum_{i=1}^{r} a_i \;>\; \frac{5}{2}(a_s - 1) + \frac{3}{8}n + \frac{5}{8}(2n - 4a_s) + n \;=\; \frac{21}{8}n - \frac{5}{2},$$

so $n < 47$. For $n < 47$ it can be directly verified that the case in question does not occur.

Next assume a_s is even. Then a_{r-1} is odd, so

$$a_{r-1} = a_v + a_u \quad \text{for some } v < u.$$

Again we need a case distinction:

1. Let $v > s$. Then the shape of the optimal addition chain is

   $$1, \ldots, a_s, \ldots, a_v, \ldots, a_u, \ldots, a_{r-1},\; n,$$

   so we have

   $$\begin{aligned} \frac{18n}{7} > S(n) \;&\geq\; S(a_s) + a_v + a_u + a_{r-1} + n \\ &\geq\; 2(a_s - 1) + a_v + a_u + a_{r-1} + n \\ &=\; 3n - 2, \end{aligned}$$

   so $n < 5$. For $n < 5$ the case in question does not occur.

2. Let $v = s$. Then the shape of the optimal addition chain is

   $$1, \ldots, a_v, \ldots, a_u, \ldots, a_v + a_u,\; 2a_v + a_u = n.$$

   Then in this addition chain the value $a_v + a_u$ can be replaced by $2a_v$, giving an addition chain for n with a smaller sum, so the addition chain was not optimal. Contradiction.

3. Let $v < s$. Then the shape of the optimal addition chain is

$$1, \ldots, a_v, \ldots, a_s, \ldots, a_u, \ldots, a_{r-1}, \ n.$$

Combining the inequalities

$$\sum_{i=1}^{s} a_i \geq S(a_s) \geq 2(a_s - 1)$$

and

$$\sum_{i=1}^{s} a_i \geq S(a_v) + a_s \geq 2(a_v - 1) + a_s$$

we obtain

$$\sum_{i=1}^{s} a_i \geq a_s - 1 + \frac{2(a_v - 1) + a_s}{2} = \frac{3a_s}{2} + a_v - 2,$$

so we have

$$\begin{aligned} \frac{18n}{7} > S(n) &\geq \frac{3a_s}{2} + a_v - 2 + a_u + a_{r-1} + n \\ &= \frac{5n}{2} + \frac{a_{r-1}}{2} - 2 \\ &\geq \frac{11n}{4} - 2, \end{aligned}$$

so $n < 12$. For $n < 12$ the case in question does not occur.

As all cases led to a contradiction, we have proved the proposition. □

Proposition 11 *Let*

$$1 = a_0, \ a_1, \ a_2, \ldots, \ a_r = n$$

be an optimal addition chain for an odd number $n > 1, n \neq 7, 11, 13, 29$, *and let* a_{r-1} *be even. Then*

$$a_{r-1} = 2 * a_{r-2}.$$

As a consequence, $n = a_{r-1} + a_{r-2} = 3 * a_{r-2}$ *is divisible by* 3.

Proof: From proposition 10 we know that $n = a_{r-1} + a_{r-2}$. Assume that

$$a_{r-1} \neq 2 * a_{r-2}.$$

Let $a_{r-1} = a_v + a_u$ with $v \leq u$. We distinguish two cases: $u < r - 2$ and $u = r - 2$.

First assume $u < r - 2$. Then we have

$$\sum_{i=1}^{r-2} a_i \geq \sum_{i=1}^{u} a_i + a_{r-2} \geq S(a_u) + a_{r-2} \geq 2(a_u - 1) + a_{r-2} \geq a_{r-1} - 2 + a_{r-2} = n - 2$$

and

$$\sum_{i=1}^{r-2} a_i \geq S(a_{r-2}) \geq \frac{5}{2}(a_{r-2}-1).$$

Multiplying the first inequality by 3/5 and the second by 2/5 and adding them gives

$$\sum_{i=1}^{r-2} a_i \geq \frac{3n}{5} + a_{r-2} - \frac{11}{5}.$$

We conclude

$$\frac{18n}{7} > \sum_{i=1}^{r} a_i \geq \frac{3n}{5} + a_{r-2} - \frac{11}{5} + a_{r-1} + n = \frac{13n}{5} - \frac{11}{5},$$

so $n < 77$. It is directly checked that for these values the case in question does not occur.

Next assume $u = r-2$. Since $a_{r-1} \neq 2 * a_{r-2}$ we have $v < u$. Since a_{r-1} is even we see that $a_u = a_{r-2}$ is odd; since $a_{r-1} = a_v + a_u$ we see that a_v is also odd. We obtain

$$\sum_{i=1}^{u} a_i \geq S(a_u) \geq \frac{5}{2}(a_u - 1)$$

and

$$\sum_{i=1}^{u} a_i \geq S(a_v) + a_u \geq \frac{5}{2}(a_v - 1) + a_u.$$

Multiplying the first inequality by 10/13 and the second by 3/13 and adding them gives

$$\sum_{i=1}^{u} a_i \geq \frac{15a_v}{26} + \frac{28a_u}{13} - \frac{5}{2}.$$

We obtain

$$\begin{aligned} \frac{18n}{7} > S(n) &\geq \frac{15a_v}{26} + \frac{28a_u}{13} - \frac{5}{2} + a_{r-1} + n \\ &= \frac{67n}{26} - \frac{5}{2}, \end{aligned}$$

so $n < 455$. For $n < 60$ the proposition is checked directly, e.g. by using table 1. For $60 < n < 455$ and $n \neq 71, 89, 191$ an addition chain with sum smaller than $\frac{67n}{26} - \frac{5}{2}$ is easily found using the construction in lemma 2 by choosing $k = 3$ or $k = 4$. For $n = 71, 89, 191$ it is checked that the addition chain constructed in this way has a sum smaller than $S(a_u, a_v) + a_{r-1} + n$ for all possible candidates for a_u and a_v. □

As a consequence, for n odd, $n > 29$ and n not divisible by 3, the number a_{r-1} in an optimal addition chain for n is always odd.

For n odd and n divisible by 3, either $a_{r-1} = 2a_{r-2}$ and $n = 3a_{r-2}$ and $S(n) = S(n/3) + 5n/3$, or a_{r-1} is odd. Both cases occur infinitely many times: the first one

for example for $n = 3^k$, the second one for example for $n = 2^{2k+1} + 1$, where the optimal addition chains are built according proposition 2.

In any case, looking for an optimal addition chain for some number n can always be restricted to looking for an optimal addition chain with a_{r-1} is odd. For this number a_{r-1} only a small variation is possible, as is shown in the next proposition.

Proposition 12 *Let n be an odd number, $n > 1$. Let*

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = n$$

be an optimal addition chain for n for which a_{r-1} is odd. Then

$$.5 * n = \frac{n}{2} < a_{r-1} < \frac{22n}{35} + 1 \approx .63 * n.$$

Proof: The first inequality is trivial, the second follows from

$$\frac{18n}{7} > S(n) \geq \sum_{i=1}^{r-1} a_i + n \geq S(a_{r-1}) + n \geq \frac{5}{2}(a_{r-1} - 1) + n.$$

□

6 Star chains

A reasonable simplification of the notion of an addition chain is the *star chain.* As in [1], a *star chain for n* is defined to be a sequence of integers

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = n$$

with the property that for all $i = 1, 2, \ldots r$ there exists an integer j with $0 \leq j < i$ and

$$a_i = a_j + a_{i-1}.$$

The motivation for star chains is that in the corresponding evaluation of x^n, the most recently computed intermediate value can always be retained in the accumulator.

Most addition chains we discussed are star chains. All addition chains in table 1 are star chains. For numbers of the shape

$$2^k * \prod_i (2^{\nu(i)} + 1)$$

we classified all optimal addition chains, and they all are star chains.

One may wonder whether all integers have optimal addition chains that are star chains. However, this is not true. For example

$$1, 2, 4, 8, 9, 16, 32, 64, 73, 137$$

is the only optimal addition chain for 137, proving that $S(137) = 345$, but the star chain for 137 with the smallest sum is

$$1, 2, 3, 4, 7, 9, 16, 32, 64, 73, 137$$

with sum 347.

For values $b_1, \ldots, b_s$ let $S^*(b_1, \ldots, b_s)$ denote the minimal sum of a star chain containing all non-zero elements of $b_1, \ldots, b_s$. Since all star chains are addition chains, we always have

$$S(b_1, \ldots, b_s) \leq S^*(b_1, \ldots, b_s),$$

and all lower bounds on $S(n)$ also hold for $S^*(n)$.

Translating upper bounds on $S(n)$ to upper bounds on $S^*(n)$ can only be done if the constructed chains are star chains. This holds for lemma 2 if $m \geq a$ and $m \geq b_1, \ldots, b_s$, and for propositions 3, 4 and 6. In proposition 5, however, the fact

$$S(m, a) \leq S(m) + S(a)$$

is used. For addition chains this is a trivial observation, but for star chains this is not; we leave as a conjecture that the similar inequality

$$S^*(m, a) \leq S^*(m) + S^*(a)$$

also holds.

Although we cannot use this inequality, we can prove a star version of proposition 5. Only the value c will be slightly worse. First we need a lemma.

Lemma 3 *Let m, a be integers with $m \geq a \geq 0$, $m \neq 0$. Then*

$$S^*(m, a) < \frac{37m}{10} + a.$$

Proof: The proof is given by induction to a. For $a = 0$ we have

$$S^*(m, a) = S^*(m) < \frac{18m}{7} < \frac{37m}{10} + a.$$

For $a > 0$ let

$$1 = a_1,\ a_2, \ldots,\ a_r = a$$

be an optimal star chain for a and m **mod** a and let

$$1 = b_1,\ b_2, \ldots,\ b_s = m \textbf{ div } a$$

be an optimal star chain for m **div** a. Then

$$1 = a_1,\ a_2, \ldots,\ a_r = a = a * b_1,\ a * b_2, \ldots,\ a * b_s = a * (m \textbf{ div } a),\ m$$

is a star chain for m and a. Here the last step is addition by m **mod** a, since

$$a * (m \textbf{ div } a) = m - (m \textbf{ mod } a).$$

Applying this equality, the induction hypothesis for a and m **mod** a, and the star version of proposition 4 for m **div** a we obtain

$$\begin{aligned} S^*(m,a) &\leq S^*(a, m \textbf{ mod } a) + a * S^*(m \textbf{ div } a) + m \\ &< \frac{37a}{10} + (m \textbf{ mod } a) + a * \frac{27((m \textbf{ div } a) - 1)}{10} + m \\ &= \frac{37m}{10} + a - \frac{17(m \textbf{ mod } a)}{10} \\ &\leq \frac{37m}{10} + a. \end{aligned}$$

□

Proposition 13 *For all integers $n > 1$ we have*

$$S^*(n) < \frac{5n}{2} + c\sqrt{n},$$

where $c = 3.9$.

Proof: Choose the integer k such that

$$2^k \leq \sqrt{n} < 2^{k+1},$$

and write $n = 2^k m + a$ with $0 \leq a < 2^k$. Then we have

$$a < 2^k \leq \sqrt{n} \leq \frac{n}{2^k} = m + \frac{a}{2^k} < m + 1,$$

so $a \leq m$. Since $\sqrt{n} < 2^{k+1}$ we obtain

$$m \leq \frac{n}{2^k} < 2\sqrt{n}.$$

By the star version of lemma 2 and lemma 3 we obtain

$$\begin{aligned} S^*(n) &\leq \frac{5n}{2} + S^*(m,a) - \frac{a}{2} - 2m \\ &< \frac{5n}{2} + \frac{37m}{10} + a - \frac{a}{2} - 2m \\ &= \frac{5n}{2} + \frac{17m}{10} + \frac{a}{2} \\ &< \frac{5n}{2} + \frac{17}{10} * 2\sqrt{n} + \frac{1}{2}\sqrt{n} \\ &= \frac{5n}{2} + 3.9\sqrt{n}. \end{aligned}$$

□

Since proposition 3 holds for star chains, propositions 7 and 8 also hold for star chains. Applying proposition 13 instead of proposition 5 we obtain a star chain version of proposition 9, in which the constant c is replaced by 3.9.

Propositions 10, 11 and 12 also hold for star chains since only proposition 3 is applied and all chains found in the verifications for small numbers in the proofs are star chains.

7 The length of optimal addition chains

What can be said about the length of optimal addition chains? Let the length of an addition chain

$$1 = a_0,\ a_1,\ a_2, \ldots,\ a_r = n$$

be defined by the number r.

The first question to ask is whether the length of an optimal addition chain is uniquely determined. It turns out that it is not; the smallest example of this phenomenon is obtained by taking $n = 145$: there are three optimal addition chains

$$1, 2, 4, 8, 9, 17, 34, 68, 77, 145$$

$$1, 2, 4, 5, 9, 18, 36, 72, 73, 145$$

$$1, 2, 3, 6, 9, 18, 36, 72, 73, 145$$

of length nine, and also three

$$1, 2, 3, 5, 6, 12, 17, 29, 58, 87, 145$$

$$1, 2, 3, 4, 7, 14, 15, 29, 58, 87, 145$$

$$1, 2, 3, 4, 7, 11, 18, 29, 58, 87, 145$$

of length ten, all of them having the optimal sum $S(145) = 364$.

Let $l_S^-(n)$ and $l_S^+(n)$ be the smallest and the greatest possible length of an optimal addition chain for n, respectively, and let $l(n)$ be the smallest possible length of an addition chain for n. Clearly we have

$$\log_2 n \leq l(n) \leq l_S^-(n) \leq l_S^+(n)$$

for all positive integers n. In section 4 it was noted that the second inequality is strict for $n = 382$, while in the above example we see that the third inequality is strict for $n = 145$.

Since the sum of a strictly increasing sequence of length r of positive integers always exceeds $r^2/2$, and $S(n)/n$ is bounded, we obtain

$$l_S^+(n) = O(\sqrt{n}).$$