Systematic Method for Determining the Number of Multiplications Required to Compute x^m, Where m is a Positive Integer

ICHIRO SEMBA*

We consider the problem of determining the number of multiplications required to compute x^m, where m is a positive integer. We propose a new systematic method (Euclid method) based on Euclid's algorithm. For a given positive integer n, the Euclid method determines the number of multiplications required to compute x^m for every integer m, $4 \leq m \leq n$, successively. The Euclid method gives the minimum number of multiplications for m such that the number of 1's in the binary representation of m is equal to or less than 4. The time required to determine the number of multiplications for every integer m, $4 \leq m \leq n$, is shown to be bounded by $cn^2 \log_2 n$, where c is some constant. Computer tests have been done for $n=1000$ and they have shown that the Euclid method gives the minimum number of multiplications for m such that $4 \leq m \leq 622$ and $624 \leq m \leq 1000$.

1. Introduction

Several algorithms for computing x^m are known. They are the binary method, the factor method and the power tree method.

The binary method is based on a binary representation of m. If m is an even number, then we calculate $x^{m/2}$ and square it to obtain x^m. If m is an odd number, then we calculate x^{m-1} and multiply it by x. Repeated application of these rules gives the binary method.

The factor method is based on a factorization of m. If $m=pq$, where p is the smallest prime factor of m and $q>1$, then we calculate x^p and then raise this quantity to the qth power. If m is prime, then we calculate x^{m-1} and multiply it by x. Repeated application of these rules gives the factor method.

The power tree method was proposed by Knuth [1, §4.6.3, Ex 5].

In this paper, we propose a new systematic method, Euclid method, based on Euclid's algorithm and compare the Euclid method with the above methods theoretically and experimentally.

The problem of computing x^m is easily reduced to addition, once we recall that $x^i x^j = x^{i+j}$. Thus, we define an addition chain for m as follows.

An addition chain for m (of length r) is a sequence of $r+1$ integers $a_0, a_1, \cdots, a_r$ such that (i) $a_0=1$, $a_1=2$, $a_r=m$ and (ii) for each i, $a_i=a_j+a_k$ for some $j \leq k < i$. Let $l(m)$ be the smallest length of addition chains for m.

Note that the length of an addition chain for m is equal to the number of multiplications required to compute x^m.

*Department of Pure and Applied Sciences, College of General Education, University of Tokyo, Komaba, Meguro-ku, Tokyo 153, Japan.

2. Euclid Method

In this section, we establish the Euclid method based on Euclid's algorithm.

Suppose that the Euclid method is applied to m ($4 \leq m < n$). We denote by $E(m)$ the length of the addition chain for m obtained by applying the Euclid method to m. The addition chain of length $E(m)$ for m is called E-addition chain for m.

We apply Euclid's algorithm to n and some p, $2 \leq p \leq n-1$, and obtain the following sequence.

$$\begin{aligned} n &= pq + p_1 && (0 < p_1 < p), \\ p &= p_1 q_1 + p_2 && (0 < p_2 < p_1), \\ p_{i-2} &= p_{i-1} q_{i-1} + p_i && (0 < p_i < p_{i-1}), \\ p_{k-2} &= p_{k-1} q_{k-1} + p_k && (p_k = 0). \end{aligned}$$

We denote by $E_p(n)$ the length of an addition chain for n constructed from the above sequence.

Four cases are considered.

Case 1. $p=2$ and $n=2q+p_1$ ($p_1=0$ or 1).

An addition chain for n, $1,2,2\cdot 2, \cdots, 2\cdot q, 2q+p_1=n$, can be constructed.

Thus, $E_2(n)=1+E(q)+e$ ($e=0$ or 1).

Case 2. $p=3$ and $n=3q+p_1$ ($p_1=0$ or 1 or 2).

An addition chain for n, $1,2,3,3\cdot 2, \cdots, 3\cdot q, 3q+p_1=n$, can be constructed.

Thus, $E_3(n)=2+E(q)+e$ ($e=0$ or 1).

We define $p_0=p$. We distinguish the E-addition chain based on whether or not the chain contains 3.

Case 3. $p>3$, $p_j>3$ ($0 \leq j < i$) and $0 \leq p_i \leq 3$ ($i \leq k$). The E-addition chain for p_{i-1} contains 3.

An addition chain for n, $1, 2, 3, \cdots, p_{i-1}, \cdots, p_{i-1}q_{i-1}, p_{i-1}q_{i-1}+p_i=p_{i-2}, \cdots, p, \cdots, pq, pq+p_1=n$, can be constructed.

Thus, $E_p(n)=E(q)+\cdots+E(q_{i-1})+E(p_{i-1})+i-1+e$ ($e=0$ or 1).

Case 4. $p>3$, $p_j>3$ $(0\le j<i)$ and $0\le p_i\le 3$ $(i\le k)$. The E-addition chain for p_{i-1} does not contain 3.

An addition chain for n, $1, 2, \cdots, p_{k-1}, \cdots, p_{k-1}q_{k-1}, p_{k-1}q_{k-1}+p_k=p_{k-2}, \cdots, p, \cdots, pq, pq+p_1=n$, can be constructed.

Thus, $E_p(n)=E(q)+\cdots+E(q_{k-1})+E(p_{k-1})+k-1$.

Our Euclid method is to test every integer p, $2\le p\le n-1$, and finds p which makes $E_p(n)$ minimum. Therefore, we have

$$E(n)=\min_{2\le p\le n-1} E_p(n) \quad (n\ge 4).$$

We define $E(1)=0$, $E(2)=1$ and $E(3)=2$.

The algorithm being described in PASCAL-like notation is given in Fig. 1. We explain the algorithm briefly.

In Fig. 1, the function $B(m)$ $(2\le m<n)$ is defined as follows.

$$B(m)=\begin{cases}1 & \text{if the E-addition chain for } m \text{ contains 3,}\\ 0 & \text{if the E-addition chain for } m \text{ does not contain 3.}\end{cases}$$

The variable min in Fig. 1 saves the minimum values $E_j(n)$ $(2\le j\le p\le n-1)$ such that the addition chain of length min for n does not contain 3. The variable min3 saves the minimum values $E_j(n)$ $(2\le j\le p\le n-1)$ such that the addition chain of length min3 for n contains 3. Therefore, if min $\ge$ min3, then we can conclude $B(n)=1$. If min $<$ min3, then we can conclude $B(n)=0$. The variable x counts the number of multiplications.

```
1.  begin
2.    E(1):=0; E(2):=1; B(2):=0; E(3):=2; B(3):=1;
3.    for m:=4 to n do begin
4.      min:=9999; min3:=9999;
5.      for p:=2 to m-1 do begin
6.        {Euclid's algorithm}
7.        nn:=m; pp:=p; qq:=nn div pp; rr:=nn mod pp;
8.        x:=0;
9.        while rr>0 do begin
10.         x:=x+1;
11.         if ((rr=1) or (rr=2) or (rr=3)) and (B(pp)=1) then
              begin
12.           xx:=x+E(pp)+E(qq);
13.           if xx<min3 then min3:=xx;
14.           goto 1
15.         end;
16.       x:=x+E(qq):
17.       nn:=pp; pp:=rr; qq:=nn div pp; rr:=nn mod pp
18.     end;
19.     x:=x+E(pp)+E(qq);
20.     if (B(pp)=0) and (x<min) then min:=x;
21.     if (B(pp)=1) and (x<min3) then min3:=x;
22.   1:
23.   end;
24.   if min3≤min then begin E(m):=min3; B(m):=1 end
25.               else begin E(m):=min; B(m):=0 end
26. end
27. end.
```

Fig. 1 Euclid method.

Example. Assume that $E(m)$ and $B(m)$ $(1\le m\le 9)$ are determined.

m	1	2	3	4	5	6	7	8	9
$E(m)$	0	1	2	2	3	3	4	3	4
$B(m)$		0	1	0	1	1	1	0	1

We will try to determine $E(10)$ and $B(10)$.

$p=2$ $\quad 10=2\cdot 5+0$ $\quad E_2(10)=1+E(5)=4$ $\quad$ min $=4$

$p=3$ $\quad 10=3\cdot 3+1$ $\quad E_3(10)=2+E(3)+1=5$ $\quad$ min3 $=5$

$p=4$ $\quad 10=4\cdot 2+2$, $4=2\cdot 2+0$ $\quad E_4(10)=E(2)+E(2)+E(2)+2-1=4$

$p=5$ $\quad 10=5\cdot 2+0$ $\quad E_5(10)=E(2)+E(5)+1-1=4$ $\quad$ min3 $=4$

$p=6$ $\quad 10=6\cdot 1+4$, $6=4\cdot 1+2$, $4=2\cdot 2+0$ $\quad E_6(10)=E(1)+E(1)+E(2)+E(2)+3-1=4$

$p=7$ $\quad 10=7\cdot 1+3$ $\quad E_7(10)=E(1)+E(7)+1=5$

$p=8$ $\quad 10=8\cdot 1+2$, $8=2\cdot 4+0$ $\quad E_8(10)=E(1)+E(4)+E(2)+2-1=4$

$p=9$ $\quad 10=9\cdot 1+1$ $\quad E_9(10)=E(1)+E(9)+1=5$

Thus, we have $E(10)=4$. Since min $=$ min3, it follows that $B(10)=1$.

3. Theoretical Results

Let $BM(n)$ be the length of the addition chain for n generated by the binary method. Let $FM(n)$ be the length of the addition chain for n generated by the factor method. We can easily obtain the following property.

Property 1. Let $n\ge 2$.
(1) $E(n)\le BM(n)$
(2) $E(n)\le FM(n)$

Let $v(n)$ be the number of 1's in the binary representation of n.

Theorem 1. For n such that $v(n)\le 4$, $E(n)=l(n)$.

Proof. For n such that $v(n)\le 3$, $E(n)$ is equal to $l(n)$, because the equation $BM(n)=l(n)$ is known and $E(n)\le BM(n)$.

Let $n=2^a+2^b+2^c+2^d$, where $a>b>c>d$. For n such that $v(n)=4$, Knuth [1,449] proved that $l(n)\ge a+3$, except in four cases for which $l(2^a+2^b+2^c+2^d)=a+2$.

Case 1. $a-b=c-d$
Case 2. $a-b=c-d+1$
Case 3. $a-b=3$, $c-d=1$
Case 4. $a-b=5$, $b-c=c-d=1$

By the fact that $BM(2^a+2^b+2^c+2^d)=a+3$ and $E(n)\le BM(n)$, it remains for us to prove that the Euclid

method detects an addition chain of length $a+2$ for each case.

Case 1. $2^a+2^b+2^c+2^d=\{(2^{c-d}+2^0)2^{b-d}+(2^{c-d}+2^0)\}2^d$

Thus, we have $E(n)=d+b-d+1+c-d+1$
$=b+c-d+2$
$=a+2$

Case 2. $2^a+2^b+2^c+2^d=\{(2^{c-d+1}+2^0)2^{b-d}+(2^{c-d}+2^0)\}2^d$

$2^{c-d+1}+2^0=(2^{c-d}+2^0)+2^{c-d}$

$2^{c-d}+2^0=(2^{c-d})+2^0$

$2^{c-d}=2^0 2^{c-d}$

Thus, we have $E(n)=d+b-d+1+1+1+c-d$
$=b+c-d+3$
$=a+2$

Case 3. $2^a+2^b+2^c+2^d=3(2^{b+1}+2^b+2^d)$

Thus, we have $E(n)=2+b+1+2$
$=b+5$
$=a+2$

Case 4. $2^a+2^b+2^c+2^d=3(2^{d+1}+2^{d+3}+2^{d+2}+2^d)$

The inside of the parenthesis reduces to Case 1.

Thus, we have $E(n)=2+d+5+2$
$=d+9$
$=a+2$

This completes the proof.

Theorem 2.

The time required to determine the number of multiplications for m $(4\leq m\leq n)$ is bounded by $cn^2 \log_2 n$, where c is some constant.

Proof. If we apply Euclid's algorithm to m and some p, $2\leq p\leq m-1$, then the algorithm requires time that is bounded by some constant times $\log_2 m$. Thus, the time required to determine $E(m)$ is bounded by some constant times $m \log_2 m$. Since $\sum_{m=4}^{n} m \log_2 m = O(n^2 \log_2 n)$, we obtain this theorem.

4. Experimental Results

Computer tests have been done for $m\leq 1000$. In the power tree method, the following 40 values are different from $l(m)$.

77	154	233	293	308	319	359	367	377	382
423	457	466	551	553	559	571	573	586	616
617	619	623	638	699	713	717	718	734	754
764	813	841	846	849	869	879	905	914	932

In the Euclid method, only one value 623 is different from $l(623)$. We have taken the values of $l(m)$ from Knuth [1,458].

Acknowledgement

We wish to thank referees for carefully reading this paper.

References

1. KNUTH, D. E. The Art of Computer Programming, 2, 2nd ed., Addison-Wesley, Reading, Mass. (1981).

(Received April 26, 1982)