International Journal of Algebra, Vol. 5, 2011, no. 6, 269 - 274

A Note on Addition Chains

Maurice MIGNOTTE

Department of Mathematics
University of Strasbourg – France
maurice.mignotte@math.unistra.fr

Amadou TALL

Departments of Mathematics and Computer Science
Cheikh Anta DIOP University of Dakar – Senegal
tallamad@hotmail.com

Abstract

Addition chains give a very easy way of computing x^n knowing x and n. The fact of having a minimal addition chain for an integer n gives the least number of multiplications needed to compute x^n. In this paper, we will present the binary method which is optimal for any integer of Hamming weight 1 or 2. We will show that if n has k digits in its binary expansion and the minimal length of all addition chains for n is $k+1$, then n has 2 as Hamming weight and we can then deduce that there exists a minimal addition chain obtained by the binary method for n.
Finally, we will show that there are exactly 4 kinds of addition chains possible for those kinds of integers
The binary method is also optimal for integers of Hamming weigh 3 but we will show that the converse is *false* in this case.

Keywords: Addition chain, Hamming weight, minimal length of an addition chain, binary method

1 Introduction:

Let's give back the definition of some important notions that are used in this paper.

Definition 1.1 *1. An addition chain for a positive integer n is a set of integers $a_0 = 1 < a_1 < a_2 < \ldots < a_r = n$ such that every element a_k can be written as sum $a_i + a_j$ of preceding elements of the set.*

2. *The integer r is the length of the chain.*

3. *We define $l(n)$ as the smallest r for which there exists an addition chain $a_0 = 1 < a_1 < a_2 < \ldots < a_r = n$.*
   There exists many ways of finding an addition chain for a positive integer n.

There are many ways of computing addition chains like the binary method, the window method,...
We will present here the binary method which is optimal for any integer n of Hamming weight less or equal than 2: this is the goal of this paper to prove this result.

Binary Method
The principle is, if $n = \sum_{i=0}^{t} \epsilon_i 2^i$ is the binary expansion of n then (with a multiplicative notation)

$$x^n = \prod_{i=0}^{t} x^{\epsilon_i 2^i} = \prod_{0 \le i \le t; \epsilon_i \neq 0}^{t} x^{\epsilon_i 2^i},$$

so that the total number of operations (here multiplications) is

$$N = t + \epsilon_0 + \cdots + \epsilon_t = \lfloor \log_2(n) \rfloor + s_2(n) - 1,$$

where $s_2(n) = \epsilon_0 + \cdots + \epsilon_t$ is the number of non zero elements in the binary expansion of $n =$ the Hamming weight of the vector $[\epsilon_0, \epsilon_1, \cdots, \epsilon_t]$. Using an easy argument one gets the very well-known lower bound

$$\ell(n) \ge \lceil \log_2(n) \rceil.$$

From these inequalities one obtains:

Theorem 1.2 *$\ell(2^k + 2^j) = k + 1$ for all $k \ge j \ge 0$.*

One can easily prove this theorem. Using the binary method to get an upper bound for $\ell(n)$ and the natural lower bound, we get the result.

Proof 1.2.1 *The natural lower bound of $\ell(n)$ is*

$$\lceil \log_2(n) \rceil \le \ell(n);$$

denoting $s_2(n)$ the Hamming weight of n which is 2 in this case, we have

$$\ell(n) \le \lfloor \log_2(n) \rfloor + s_2(n) - 1.$$

Hence,

$$k < \ell(n) \le k + 1.$$

This leads to the following:

2 Main Results

Question: If $n > 2^k$ and $\ell(n) = k + 1$, is it true that $n = 2^k + 2^j$ for some $j \leq k$? The answer to this question is *yes*. This is the main result of the present paper.

Theorem 2.1 *For any integer $n > 2^k$ whith $k \in \mathbf{N}$, if $\ell(n) = k + 1$ then $n = 2^k + 2^j$ for some $j \leq k$.*

Proof 2.1.1 *By hypothesis:*

$$2^k < n = u + v, \quad u \geq v, \quad \ell(n) = k + 1.$$

Thus,

$$u > 2^{k-1}, \quad \ell(u) = k$$

and, by induction,

$$u = 2^{k-1} + 2^i.$$

- *If $u \geq 2^k$ then $u = 2^k$ and we get the unique minimal chain*

$$\mathcal{C} = (1, 2, 4, \ldots, 2^{k-1}, 2^k, n), \quad n = 2^k + 2^i.$$

- *if $u < 2^k$ then $i \leq k - 2$,*

$$u \leq 2^{k-1} + 2^{k-2}, \quad v > 2^{k-2}, \quad n < 2^{k+1}.$$

– *If n is odd then $u > v$ and $\ell(v) = k - 1$, $v = 2^{k-2} + 2^h$ (by induction) with $h \leq k - 2$.*

— *If u is odd, then $u = 2^{k-1} + 1$ and $v = 2^{k-1}$. Hence the chain*

$$\mathcal{C} = (1, 2, 4, \ldots, 2^{k-2}, 2^{k-1}, 2^{k-1} + 1, 2^k + 1), \quad n = 2^k + 1.$$

— *If u is even, $u = 2^{k-1} + 2^i$, $v = 2^{k-2} + 1$ (necessarily) which implies $u = 2^{k-1} + 2^{k-2}$ and $n = u + v = 2^k + 1$. But $u \leq 2v$, hence $k - 2 = 1$ and here*

$$\mathcal{C} = (1, 2, 3, 6, 9).$$

– *If n is even.*

— *If $u = v$ then*

$$\mathcal{C} = (1, \ldots, 2^{k-1} + 2^i, 2^k + 2^{i+1}), \quad n = 2^k + 2^{i+1}.$$

— *If* $u > v$ *then* $u = 2^{k-1} + 2^i$, $i \leq k-2$ *and* $\ell(v) = k-1$, $v = 2^{k-2} + 2^h$, $h \leq k-2$; $\mathcal{C} = (1, \ldots, v, u, u+v)$. *And we get*

$$u + v = 2^{k-1} + 2^i + 2^{k-2} + 2^h = n > 2^k.$$

This implies $\max(h, i) = k-2$. *If* $h = k-2$ *then* $v = 2^{k-1}$ *and*

$$\mathcal{C} = (1, 2, 4, \ldots, 2^{k-2}, 2^{k-1}, 2^{k-1} + 2^i, 2^k + 2^i), \quad n = 2^k + 2^i.$$

The last case is $h < k-2$, *then* $u = 2^{k-1} + 2^{k-2}$, $v = 2^{k-2} + 2^h$. *But, since* $u \leq 2v$, *we get* $h = k-3$ *and*

$$\mathcal{C} = (1, \ldots, 2^{k-2} + 2^{k-3}, 2^{k-1} + 2^{k-2}, 2^k + 2^{k-3}), \quad n = 2^k + 2^{k-3},$$

which ends the proof.

Moreover, this proof gives a complete recursive description of the possible minimal additions-chains for n. As an instructive example, let's take $n = 18 = 2^4 + 2$. The possible addition chains are:

$$\mathcal{C}_0 = (1, 2, 4, 8, 16, 18), \quad \mathcal{C}_1 = (1, 2, 4, 8, 10, 18), \quad \mathcal{C}_2 = (1, 2, 4, 6, 12, 18),$$

$$\mathcal{C}_3 = (1, 2, 3, 6, 9, 18), \quad \mathcal{C}_4 = (1, 2, 3, 6, 12, 18),$$

$$\mathcal{C}_5 = (1, 2, 4, 5, 9, 18), \quad \mathcal{C}_6 = (1, 2, 4, 8, 9, 18).$$

One can see that for $\mathcal{C}_2$ and $\mathcal{C}_4$, we have $18 = u+v$ where $v = 6$ and $u = 12$. And for $\mathcal{C}_3$, $\mathcal{C}_5$ and $\mathcal{C}_6$, we have $u = v = 9$.

In summary, we can say that for an integer $n > 2^k$ such that $l(n) = k+1$, we have a minimal addition chain for n in one of this form:

(i) $(u = 2^k)$
For this case,

$$\mathcal{C} = (1, 2, 4, \ldots, 2^{k-1}, 2^k, 2^k + 2^j).$$

(ii) $(u < 2^k$ and $u = v)$
Then, one can see that $u = v = 2^{k-1} + 2^{j-1}$ and we have:

$$\mathcal{C} = (1, \ldots, 2^{k-1} + 2^{j-1}, 2 \cdot (2^{k-1} + 2^{j-1})).$$

(iii) ($u < 2^k$ and $v < u$)
For this last case, $v = 2^{k-1}$ and $u = 2^{k-1} + 2^j$. And so, the addition chain $\mathcal{C}$ is:

$$\mathcal{C} = (1, 2, 4, \ldots, 2^{k-2}, 2^{k-1}, 2^{k-1} + 2^j, 2^{k-1} + 2^{k-1} + 2^j)$$

or $v = 2^{k-2} + 2^j$ and $u = 2^{k-1} + 2^{k-2}$, and then,

$$\mathcal{C} = (1, \ldots, 2^{k-2} + 2^j, 2^{k-1} + 2^{k-2}, 2^k + 2^j).$$

Corollary 2.2 *If $2^k < n < 2^{k+1}$ and the Hamming weight of n is 3 then $\ell(n) = k + 2$ (value obtained by the binary method).*

Remark: The "converse" of the corollary is false. The set of numbers

$$\{n = 15 \times 2^j; j \geq 0\},$$

furnishes an infinite list of examples of numbers with

$$5 + j = \ell(n) < \lfloor \log_2(n) \rfloor + s_2(n) - 1 = 7 + j.$$

3 Small list of false conjectures related to addition chains

(i) $\ell(2n) = \ell(n) + 1$
Computer calculation have shown that it isn't true. We have $\ell(n) = \ell(2n)$ for some integers n like 191, 701, 743, 1111, $23 \cdot 2^5 + 7$. This leads to another conjecture which is:

(ii) $\ell(2n) \geq \ell(n)$
Indeed, this inequality may be false. Kevin R. Hebb has shown that $\ell(n) - \ell(mn)$ can be arbitrarily large for all fixed integers m not a power of 2. Moreover, Neil Clift has found that for $n = 375404703$, we have: $\ell(n) = 35 > 34 = \ell(2n)$;

(iii) $\ell(n) = \ell^*(n)$ where $\ell^*(n)$ is the minimal length of all star addition chains of n. It has been proven that $\ell(n) \leq \ell^*(n)$ for all integer n.

Nevertheless, we propose the following

Conjecture : If p is a prime number such that $n = 2^p - 1$ is prime (Mersenne numbers), then

$$\ell(n) = \max\{\ell(m);\ m \leq n\}.$$

We verified that this conjecture is true for $2 \leq p \leq 7$.

One can also ask

Question : Is this conjecture true for any $n = 2^k - 1$?

The answer to this question is *no*: for $k = 8$, $n = 255$ and $\ell(n) = 10$ whereas $\ell(254) = 11$.

References

[1] E. G. Thurber, The Scholz-Brauer problem on addition chains, Pacific J. Math., **49** (1973), p. 229–242.

[2] Edward G. Thurber, "Efficient Generation of minimal length addition chains", (1999).

[3] Donald Knuth/Addison-Wesley The Art of Computer Programming, Volume 2, Seminumerical algorithms, p. 441–466, (1980).

[4] Sander van der Kruijssen, Addition Chains efficient computing of powers -Bachelor project / , (2007).

Received: October, 2010