International Journal of Applied Mathematical Research, 2 (1) (2013) 76-83

www.sciencepubco.com/index.php/IJAMR

Efficient computation of addition-subtraction chains using generalized continued Fractions

Amadou Tall*, Ali Yassin Sanghare

African Institute for Mathematical Sciences – Senegal
**Corresponding author E-mail: amadou.tall@aims-senegal.org*

Abstract

The aim of this paper is to present a new way of computing short addition-subtraction chains using the generalized continued fractions where subtraction is allowed. We will recover the most used ways of getting addition-subtraction chains. This method is not always optimal but gives minimal chains that are easy to compute.

Keywords: *addition-subtraction chains; non-adjacent form; scalar multiplication; double-and-add method; vector chains; continued fractions; Euclidean algorithm.*

1 Introduction

Decreasing the number of multiplications needed to compute x^a when a is a big integer is a very serious problem of computation. And the addition chains give the best ways to achieve that aim. Also, the problem of finding a minimal addition chain is known to be NP–complete [10, 11, 12]. Euclidean algorithm is a polynomial algorithm (and is very important). It is used to get the continued fraction expansion of $\frac{a}{b}$, $a, b \in N$ and it is used in [3, 5] to get many of the known ways of computing addition chains.

In this paper, we will use the generalized Euclidean algorithm to have a generalized continued fraction and from that one, we will recover most of the known ways of getting addition-subtraction chains.

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 called the length of the chain.

3. We define $l(n)$ as the smallest r for which there exists an addition chain $\{a_0 = 1 < a_1 < a_2 < \ldots < a_r = n\}$ for n.

There exists many ways of finding an addition chain for a positive integer n. We can cite the classical binary method, the window method and the factor method. And many of those methods were recovered in [3, 5] using the continued fraction expansion of $\frac{n}{k}$.

1.1 Continued fractions

Let n be an integer and $k \in \{2,\ 3,\ \ldots,\ n-1\}$,
a continued fraction expansion of $\frac{n}{k}$ is:

$$\frac{n}{k} = a_r + \cfrac{1}{a_{r-1} + \cfrac{1}{\ddots + \cfrac{1}{a_2 + \cfrac{1}{a_1}}}}$$

Followong the non-usual notation of [3, 5], we denote the continued fraction expansion of $\frac{n}{k}$ by $[a_1,\ a_2,\ \ldots,\ a_{r-1},\ a_r]$.

The semi-continuants of this continued fraction Q_i are:

$$Q_0 = \gcd(n,k), \qquad Q_1 = Q_0 a_1 \qquad \text{and} \qquad Q_i = Q_{i-1}a_i + Q_{i-2} \quad \text{for } 2 \le i \le r.$$

By construction, we can see that $Q_r = n$.

Example 1.2 *Let $n = 86$ and $k = 10$, the continued fraction expansion of $\frac{86}{10}$ is $[2,\ 1,\ 1,\ 8]$, and we have:*

$$Q_0 = 2,\ Q_1 = 4,\ Q_2 = 6,\ Q_3 = 10,\ Q_4 = 86,$$

the way of computing the Q_is gives an addition chain for n,

$$C = \{1,\ 2,\ 4,\ 6,\ 10,\ 20,\ 40,\ 80,\ 86\}.$$

The method of computing short addition chains for n based on the continued fraction expansion of $\frac{n}{k}$ is well explained in [3, 5].

1.2 Addition-subtraction chains

Definition 1.3 *1. A sequence $\{1 = a_0,\ a_1,\ \ldots,\ a_l = n\}$ is called an addition-subtraction chain for an integer n if and only if:*

For every integer $i \in [1..l]$, there exist j and k with $0 \le j, k < i$ such that

$$a_i > 0 \ \text{ and } a_i = a_j + a_k \ \text{ or } a_i = a_j - a_k.$$

2. The integer l is called the length of the chain.

3. We define $l^-(n)$ as the smallest l for which there exists an addition-subtraction chain $\{a_0 = 1 < a_1 < a_2 < \ldots < a_l = n\}$ for n.

Example 1.4 *The sequence $\{1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 31\}$ is an addition-subtraction chain for 31.*

There exists many ways of finding an addition-subtraction chain for a positive integer n. In this part, we will give two ways of getting addition-sutraction chains for n.

1.2.1 Factor Method

Theorem 1.5 *Let c_1 and c_2 be addition-subtraction chains respectively for n_1 and n_2. Then $c_1 \otimes c_2$ is an addition-subtraction chain for $n_1 \cdot n_2$ where $\otimes$ is* defined *as follows:*
if $c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\}$ and $c_2 = \{b_0,\ b_1,\ \ldots,\ b_l\}$, then

$$c_1 \otimes c_2 = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r \cdot b_1,\ a_r \cdot b_2,\ \ldots,\ a_r \cdot b_l\}.$$

The practical idea of this theorem is to have an addition-subtraction chain for n by using the smallest divisor of n greater than 1 ($\neq n$) when it exists, and to work with $n-1$ if n is prime. That leads to the factor strategy that is presented later in this paper.

1.2.2 Non-adjacent form

A w–non-adjacent form (w–NAF) of length r for an integer n is a sequence of digits $(d_{r-1} \cdots d_0)$ with $|d_i| < w$ such that

$$n = \sum_{i=0}^{r-1} d_i b^i$$

and

$$d_i \cdot d_{i+1} = 0 \quad \forall i.$$

It has been proved [13] that each integer has exactly one 2-NAF representation. More importantly, it's proved that the 2–NAF minimizes the Hamming weight among all the binary signed-digit representations. That gives to the NAFs, the particularity of being suitable for fast exponentiations.

Example 1.6 *For* $e = (11101)_2$, *we get* $NAF(e) = (100\bar{1}01)_{\bar{2}}$.

Here is an algorithm [5] to get the 2–NAF which is also called the Non-adjacent form of any integer n using its binary expansion.

Algorithm 1 nonAdjacentForm (e)

Require: e : integer
Ensure: the non–adjacent form of e

```
i ← 0
while (i < λ2(e) − 1) do
  if (e_i == 1 et e_{i+1} == 1) then
    e_i ← 1̄
    i ← i + 1
    while (e_i == 1) do
      e_i ← 0
      i ← i + 1
    end while
    e_i ← 1
  end if
end while
```

and, the addition-subtraction chain for an integer n is obtained using the non-adjacent form by the same way than in the binary method. We have to look at the digit and add when it is equal to 1, subtract when it is -1.

2 Generalized continued fractions

Let n be an integer and $k \in \{2,\ 3,\ \ldots,\ n-1\}$.
A generalized continued fraction expansion of $\frac{n}{k}$ where subtraction is allowed, is in our case:

$$\frac{n}{k} = a_r + \cfrac{b_{r-1}}{a_{r-1} + \cfrac{b_{r-2}}{\ddots + \cfrac{b_2}{a_2 + \cfrac{b_1}{a_1}}}}$$

where $b_i \in \{1, -1\}$.

Theorem 2.1 *1. In the classical case,* b_i *is always equal to* 1.

2. Our generalized continued fraction is obtained easily with the generalized euclidean algorithm.

We denote this generalized continued fraction expansion of $\frac{n}{k}$ by $[b_1a_1,\ b_2a_2,\ \ldots,\ b_{r-1}a_{r-1},\ a_r]$.

Example 2.1 *Let's take* $n = 55$ *and* $k = 28$*, then* $55 = 1 * 28 + 27$ *is the classical Euclidean division and gives us this continued fraction expansion*

$$\frac{55}{28} = 1 + \frac{27}{28} = [27,\ 28],$$

and the generalized Euclidean division gives us $55 = 2 * 28 - 1$ *and the generalized continued fraction is*

$$\frac{55}{28} = 2 - \frac{1}{28} = [-28,\ 2].$$

Let's define the generalized semi-continuants of this continued fraction Q_i by:

$$\begin{aligned} Q_0 = \gcd(n,k), \quad & Q_1 = Q_0 \cdot a_1, \\ Q_i = Q_{i-1}a_i + b_{i-1}Q_{i-2}, \quad & \forall 2 \leq i \leq r. \end{aligned}$$

By construction, we can see that $Q_r = n$.

Theorem 2.1 *Let's prove by induction that, if* $Q_o = \gcd(n,k)$ *then*

$$Q_r = n = Q_o \cdot N \text{ and } Q_{r-1} = k = Q_0 \cdot K.$$

Let

$$\frac{n}{k} = \frac{N}{K} = a_2 + \frac{b_1}{a_1}$$

then, $\frac{N}{K} = \frac{a_2a_1+b_1}{a_1}$ *and we know that*

$$Q_1 = a_1 \cdot Q_0 = Q_0 \cdot K = k$$

and

$$Q_2 = a_2Q_1 + b_1Q_0 = a_2a_1Q_0 + b_1Q_0 = Q_0 \cdot N = n.$$

Now, let's suppose that the relation holds until $r-1$ *and*

$$\frac{n}{k} = \frac{N}{K} = a_r + \cfrac{b_{r-1}}{a_{r-1} + \cfrac{b_{r-2}}{\ddots + \cfrac{b_2}{a_2 + \cfrac{b_1}{a_1}}}}$$

then $\frac{N}{K} = a_r + \frac{b_{r-1}}{\frac{n_0}{k_0}}$*, and so*

$$\frac{N}{K} = \frac{a_rn_0 + b_{r-1}k_0}{n_0};$$

thanks to the reccursion, we can conclude that $n_0 = \frac{Q_{r-1}}{Q_0}$ *and* $k_0 = \frac{Q_{r-2}}{Q_0}$*, and it means that*

$$n_1 = \frac{n}{Q_0} = a_r\frac{Q_{r-1}}{Q_0} + b_{r-1}\frac{Q_{r-2}}{Q_0} = \frac{Q_r}{Q_0}.$$

And now, let $C(d)$ be an addition-subtraction chain for $d = \gcd(n,k)$ and for $i \in [1..r]$, let $C_i = C(u_i)$ be some addition-subtraction chain for u_i.

Let's define this new sequence of addition-subtraction chains X_i for all $i \in [1..r]$:
$X_0 = C(d), \quad X_1 = X_0 \otimes C_1$, and for all $i \in [2..r]$

$$X_i = \begin{cases} (X_{i-1} \otimes C_i) \oplus Q_{i-2} \text{ if } b_{i-1} > 0, \\ (X_{i-1} \otimes C_i) \ominus Q_{i-2} \text{ if } b_{i-1} < 0, \end{cases}$$

where $\otimes$, $\oplus$ and $\ominus$ are defined this way:

Definition 2.2 *1. if* $c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\}$ *and* $c_2 = \{b_0,\ b_1,\ \ldots,\ b_l\}$, *then*

$$c_1 \otimes c_2 = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r \times b_1,\ a_r \times b_2,\ \ldots,\ a_r \times b_l\},$$

2. if $c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\}$ *and* $m \in c_1$, *then*

$$c_1 \oplus m = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r + m\},$$

3. if $c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\}$ *and* $m \in c_1$, *then*

$$c_1 \ominus m = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r - m\}.$$

By this definition, we can see that these three operations give new addition-subtraction chains.

Theorem 2.2 *1. Notice that, in the above definition, we need that* m *always appears in the chain* c_1.

2. X_r *is an addition-subtraction chain for* n *of length* $\ell^-(C(d)) + r - 1 + \sum_{i=1}^{r} \ell^-(c_i)$.

The choice of k is very important if we want to have short addition-subtraction chains, and to our knowledge, there is no good heuristics known way to choose k, this point remains mysterious. The known ways of choosing k are the *strategies*.

Definition 2.3 *A strategy is a function* γ *that determines for every integer* n *some non empty subset of* $\{2, 3, \ldots, n-1\}$.

Here are a few examples, and we will see how to get addition-subtraction chains with some of them.

(1) **Total Strategy**

$$t(n) = \{2,\ 3,\ \ldots,\ n-1\}.$$

(2) **Binary Strategy**

$$\beta(n) = \left\{ \left\lfloor \frac{n}{2} \right\rfloor \right\}.$$

The chains obtained with the binary stratedy are exactly the classical binary chains. With the following modification, we have the chains obtained using the Non-adjacent form.

(3) **Modified-Binary Strategy**

$$\beta_2(n) = \left\{ \left\lfloor \frac{n}{2} \right\rfloor \text{ if } \frac{n}{2} \text{ is even}, \quad \left\lfloor \frac{n+1}{2} \right\rfloor \text{ otherwise} \right\}.$$

With this strategy, we have the addition-subtraction chains obtained with the non-adjacent form, and we gain one step (in the length of the chain) when $n = 3 * 2^k + x$ where $\log_2(x) < k$.

Example 2.4 *Let's take* $n = 55$, *then* $\beta_2(n) = 28$ *and the gcf is* $[-28,\ 2]$.
$\gcd(55, 28) = 1$, *then we have*

$$Q_0 = 1,\ Q_1 = 28 \text{ and } Q_2 = 2 \cdot 28 - 1 = 55,$$

and after computing the sequence of addition-subtraction chain, we obtained this last chain

$$\{1,\ 2,\ 4,\ 8,\ 7,\ 14,\ 28,\ 56,\ 55\}.$$

(4) **Factor Strategy**

$$\pi(n) = \begin{cases} \{n-1\}, & \text{if } n \text{ is prime;} \\ \{n-1,\ q\}, & \text{otherwise, where } q \text{ is the smallest prime dividing } n. \end{cases}$$

The factor strategy gives us the factor addition chains that we were talking about below. (need to modify it to have some factor addition-subtraction chains)

We will get the factor addition-subtraction chains using this new strategy. This strategy uses a primaly test and/or a factorization algorithms, and so the factor strategy isn't suitable all the time.

(5) **Square root Strategy**

$$\beta(n) = \left\{ \lfloor \sqrt{n} \rfloor \right\}$$

Example 2.5 *Let* $n = 55$*, then* $\beta(n) = 7$ *and the gcf is* $[-8,\ 7]$.
Then $\gcd(55, 7) = 1$*, and we have*

$$Q_0 = 1,\ Q_1 = 8 \text{ and } Q_2 = 7 \cdot 8 - 1 = 55,$$

and after computing the sequence of addition-subtraction chain, we obtained this last chain

$$\{1,\ 2,\ 4,\ 8,\ 16,\ 24,\ 48,\ 56,\ 55\}.$$

Many other strategies exist and aren't studied in this paper.

Definition 2.6 *An addition-subtraction chain c for n is called a gcf–chain when it exists an integer k such that the generalized continued fraction expansion of* $\frac{n}{k}$ *allows to get c using the method describe above.*

Now, we will give an algorithm to have gcf–chains for n.

3 Algorithm

We will create a first algorithm $MinChain(n,\ \gamma)$ wich will allow us to have a minimal gcf–chain for Q_0 and for all the u_i using the strategy γ. From those chains, we will construct another algorithm $Chain(n, k)$ which will get the generalized continued fraction expansion of $\frac{n}{k}$ and obtain all the gcf–chains X_i, we will return X_r which is a gcf–chain for n.

Algorithm 2 MinChain$(n,\ \gamma)$

Require: n : integer, γ: a strategy
Ensure: a sequence of integers that is a gcf–chain for n

```
if (n = 2^a) then
    chain = 1, 2, 2^2, ..., 2^a
else
    if (n = 3) then
        chain = 1, 2, 3
    else
        choose k ∈ γ(n) such that Chain(n, k) is minimal
        chain = Chain(n, k)
    end if
end if
return chain
```

and now, here is the algorithm to construct a gcf–chain for n,

Algorithm 3 Chain($n,\ k,\ \gamma$)

Require: $n,\ k$: integers, γ: a strategy
Ensure: a sequence of integers that is a gcf–chain for n

$gcf = [u_1,\ u_2,\ \ldots,\ u_r]$ the generalized continued fraction expansion of $\frac{n}{k}$
$Q_0 = \gcd(n, k)$; $Q_1 = |u_1| \cdot Q_0$
$X_0 = MinChain(Q_0, \gamma)$; $X_1 = X_0 \otimes MinChain(|u_1|)$
for $i = 2$ to r **do**
  $Q_i = |u_i| Q_{i-1} + sign(u_{i-1}) Q_{i-2}$
  $X_i = X_{i-1} \otimes MinChain(|u_i|)$
  if $(u_{i-1} < 0)$ **then**
    $X_i = X_i \ominus Q_{i-2}$
  else
    $X_i = X_i \oplus Q_{i-2}$
  end if
end for Return X_r

Those algorithms were implemented in gp-pari by the author and tested. Now we will study the complexity of those gcf–chains obtained with the algorithms above according to the chosen strategy γ. For that, we will give this definition:

Definition 3.1 *Let $n,\ k$ be integers $(n > k)$ and lambda a strategy, we denote by:*

1. *$\ell^-(n, \gamma)$ the length of a shortest gcf–chain for n according to γ,*
2. *$L^-(\{n,\ k\}, \gamma)$ tht length of a shortest gcf–chains for n containing k and obtained through the generalized continued fraction expansion of $\frac{n}{k}$.*

We have:

$$\ell^-(n,\gamma) = \begin{cases} a \text{ if } n = 2^a, \\ a+1 \text{ if } n = 2^a \pm 2^b,\ a > b \\ \min\{L^-(\{n,\ k\}, \gamma),\ k \in \gamma(n)\} \text{ otherwise} \end{cases}$$

and here is a definition by induction of $L^-()$

$$L^-(\{n,\ k\},\gamma) = \begin{cases} L^-(\{k\},\gamma) + \ell^-(q,\gamma) \text{ if } r = 0, \\ L^-(\{n,\ k\},\gamma) + \ell^-(q,\gamma) + 1 \text{ if } r \in \{1,\ 2\}, \\ L^-(\{k,\ r\},\gamma) + \ell^-(q,\gamma) + 1 \text{ otherwise} \end{cases}$$

with $n = kq \pm r$ and $0 \leq r < \frac{k}{2}$.

Now, we will deduce from the last result that

$$L^-(\{n,\ k\},\gamma) = \begin{cases} \ell^-(k,\gamma) + \ell^-(q,\gamma) \text{ if } n = kq, \\ \ell^-(\{k,\ r\},\gamma) + \ell^-(q,\gamma) + 1 \text{ if } n = kq \pm r \text{ with } 0 < r < \frac{k}{2} \end{cases}$$

because every chain for k contains 1 and 2. Now, we can see that the complexity of computing a $\ell^-(n, \gamma)$ for an integer n using a strategy γ is $O(xxxx)$.

4 Conclusion

In this paper, we have presented new computationally easy ways of getting addition-subtraction chains that recover most of the known ways (binary, non-adjacent form, factor method, ...). Although, one can think about using the generalized continued fraction to recover the window method. Addition-subtraction chains can give fast, efficient and secure scalar multiplication on elliptic curves, which are very important in elliptic curve cryptography. It will be interesting to investigate possible scalar multiplications based on this new ways. A more precise value of the complexity can also be found.

5 Acknowledgements

The author is happy to acknowledge the endless help of Professor Maurice Mignotte, this work was started during my visit to the university of Strasbourg funded by the Ibni Prize.

References

[1] François Morrain, Jorge Olivos Speeding up the computation on an elliptic curve using addition-subtaction chains, Informatique théorique et applications 24, (6) (1990) 531-543.

[2] Peter L. Montgomery. Evaluating recurrences of form $X_{m+n} = f(X_m,\ X_n,\ X_{m-n})$ via Lucas Chains, January 1992.

[3] F. Bergeron, J. Berstel, S. Brlek and C. Duboc, Addition chains using continued fractions, journal of algorithms 10, p 403-412, 1989

[4] F. Bergeron, J. Berstel and S. Brlek, Efficient computation of addition chains, Journal de théorie des nombres de Bordeaux 6, p 21-38, 1994

[5] Hugo Volger. Some results on addition-subtraction chains, Information Processing Letters 20 (3) (8 April 1985) 155-160.

[6] Maurice Mignotte, Amadou Tall, A note on addition chains, International Journal of Algebra 5 (6) (2011) 269 - 274.

[7] Tall Amadou, A generalization of Lucas addition chains, Bulletin Mathématique de la Roumanie Tome 55 (103) (1) (2012) 79 - 93.

[8] K. Koyama, Y Tsuruoka, Speeding elliptic cryptosystems using a signed binary window method, Advances in cryptology 740 (1992) 345 - 357.

[9] CY. Sakari, K. Sakurai, Efficient scalar multiplication on elliptic curve with direct computations of several doublings, IEICE Transactions Fundamentals E84-A(1) (2001) 120-129.

[10] P. Downey, B. Leong and R. Sethi; "computing sequences with addition chains"', SIAM journal on Computing, 10 (3), p 638-646, 1981

[11] Y. Yacobi, "Exponentiating faster with addition chains", Lecture notes in computer science, Volume 473/1991, p 222 - 229, Bellcore, 1991

[12] A. Flammenkamp "Integers with a Small Number of Minimal Addition Chains", Discrete Mathematics V. 205 1999 pp 221-227

[13] T. Takgi, D. Reis, S. Yen and B. Wu. Radix-r Non-Adjacent Form and Its Application to Pairing-Based Cryptosystem. IEICETRANS. Fundamentals,VOL. E 89-A,NO. 1 January 2006

[14] D. Bleichenbacher and A. Flammenkamp "An Efficient Algorithm for Computing Shortest Addition Chains", submitted 1997 to SIAM Journal of Discrete Mathematics.