sciendo

TATRA MOUNTAINS
Mathematical Publications
DOI: 10.2478/tmmp-2023-0010
Tatra Mt. Math. Publ. **83** (2023), 131–144

ON THE CONSTRUCTION OF SHORT ADDITION-SUBTRACTION CHAINS AND THEIR APPLICATIONS

Moussa Ngom — Amadou Tall*

Université Cheikh Anta Diop de Dakar, SENEGAL

ABSTRACT. The problem of computing x^n efficiently, such that x and n are known to be very interesting, specially when n is very large. In order to find efficient methods to solve this problem, addition chains have been much studied, and generalized to addition-subtraction chains. These various chains have been useful in finding efficient exponentiation algorithms. In this paper, we present a new method to recover all existing exponentiation algorithms. It will be applied to design a new fast exponentiation method.

1. Introduction and background

Let n be a positive integer and x an element of a multiplicative group (resp. additive group). The exponentiation of x to the n denoted x^n (resp. nx) is defined as follows

$$x^n = \underbrace{x \times x \cdots \times x}_{n \text{ times}} \quad \text{and} \quad nx = \underbrace{x + x + \cdots + x}_{n \text{ times}}.$$

Exponentiation is a key operation. It is good to investigate techniques for doing such operation, specially when n get large. Finding fast exponentiation methods gain interest. The best known tool is the addition chains.

2020 Mathematics Subject Classification: 11Yxx, 11Bxx, 11T71.
Keywords: addition-subtraction chains, non-adjacent form, strategy, minimal length of chain, generalized continued fractions, Euclidean algorithm.

* The corresponding author.

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

Example. The sequence $\{1,\ 2,\ 4,\ 5,\ 10,\ 20,\ 40,\ 41\}$ is an addition chain for 41.

And we can compute x^{41} with 7 multiplications, instead of 41 as stated in the definition.

$$x,\ x^2,\ x^4 = (x^2)^2, \quad x^5 = x^4 \times x, \quad x^{10} = (x^5)^2, \quad x^{20},\ x^{40},\ x^{41} = x^{40} \times x.$$

Definition 1.2. The integer r is called the length of the chain.

Definition 1.3. We define $\ell(n)$ as the smallest r for which there exists an addition chain

$$\{a_0 = 1 < a_1 < a_2 < \cdots < a_r = n\} \quad \text{for } n.$$

A chain for n of length $\ell(n)$ is called a minimal chain for n.

There exist several methods to compute addition chains. A very popular one is the fast exponentiation method which is based on the binary expansion of n. We will describe it later. The problem of finding a minimal addition chain is known to be NP-complete [3, 7, 9]. We will present other methods that can be faster than the binary method.

Euclidean algorithm is a polynomial algorithm used to obtain the continued fraction expansion of $\frac{a}{b}$, $a, b \in \mathbb{N}$. It is used in [4,5] to recover many of the known ways of computing addition chains.

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

Theorem 1.4. *Let a and b be two positive integers. There exist a unique couple $(q, r) \in \mathbb{N} \times \mathbb{Z}$ such that*

$$a = bq + r \quad \textit{with} \quad -\frac{b}{2} < r < \frac{b}{2}.$$

We will then design a new fast exponentiation method.

This paper is structured as follows. In the next section, we will remind the notion of addition (and addition-subtraction) chains. We will then explain the most used methods to construct such chains. The next section will be devoted to the continued fractions, a key tool in the development of our algorithm. The theory of our approach will then be presented. Finally, we will compare several strategies.

1.1. Addition-subtraction chains

1.2. Definitions

We now define an addition-subtraction chain as follows:

Definition 1.5. 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

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

The integer l is called the length of the chain.

Definition 1.6. We define $\ell^-(n)$ as the smallest l for which there exists an addition-subtraction chain

$$\{a_0 = 1 < a_1 < a_2 < \cdots < a_l = n\} \quad \text{for } n.$$

Such chain is called a minimal addition-subtraction chain for n.

Example. The sequence

$$\{1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 63\}$$

is an addition-subtraction chain for 63.

Addition-subtraction chains can be shorter than addition chains. There give shorter minimal chains for infinitely many infinite sets of integers. For example, there exist infinitely many integers n satisfying

$$\ell(2^n - 1) = \ell(n) + n - 1 < n + 1 = \ell^-(2^n - 1).$$

1.3. Some methods of finding addition-subtraction chains

There are many ways of computing addition-subtraction chains for a positive integer n. In this section, we will give some of them.

1.3.1. The binary method (double-and-add)

Let $n = \sum_{i=0}^{t} \epsilon_i 2^i$ be the binary expansion of n, then

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

so, the total number of operations (steps) is

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

where $v(n) = \epsilon_0 + \cdots + \epsilon_t$ is the Hamming weight of n (which corresponds to the number of "1"s in the binary expansion of n).

Here is an example of computing addition chain for n using the binary method.

EXAMPLE.

(1) $n = 13 = (1101) = 8 + 4 + 1$.
An addition chain for 13 using the binary method is $\{1,\ 2,\ 3,\ 6,\ 12,\ 13\}$.

$$\begin{aligned} 13 &= 12 + 1 \\ &= (6 * 2) + 1 \\ &= \big((3 * 2) * 2\big) + 1, \\ 13 &= \Big(\big((2 + 1) * 2\big) * 2\Big) + 1, \end{aligned}$$

then

$$x^{13} = x^{((((2+1)*2)*2)+1)} = x * \left(\left(x^{2+1}\right)^2\right)^2$$

meaning that we will successively compute

$$x,\ x^2,\ x^3,\ x^6,\ x^{12},\ x^{13}.$$

The binary method is also called the "double-and-add" algorithm. We will better illustrate it with the following example.

(2) Let $n = 53$. Its binary expansion is 110101. We will read the bits from left to right. There will be a doubling every time, and a +1 every time when the bit is equal to 1.

- $a_0 = 1$ and $a_1 = 2a_0 = 2$, the second bit is 1(1**1**0101) so $a_2 = a_1 + 1 = 3$, and
- $a_3 = 2a_2 = 6$, the next bit is 0 (11**0**101) leading to $a_4 = 2a_3 = 12$.
- The following bit is 1 (110**1**01) so $a_5 = a_4 + 1 = 13$ and $a_6 = 2a_5 = 26$.
- The next one is 0 (1101**0**1) so $a_7 = 2a_6 = 52$.
- The last bit is 1 (11010**1**) so $a_8 = a_7 + 1 = 53$.

Finally, the corresponding addition chain is $\{1, 2, 3, 6, 12, 13, 26, 52, 53\}$. Again again

$$53 = \Big(2\Big(2\big(2(2(2 + 1)))\big) + 1\Big)\Big) + 1.$$

1.3.2. The non-adjacent form

DEFINITION 1.7. 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

$$n = \sum_{i=0}^{r-1} d_i b^i \quad \text{and} \quad d_i \cdot d_{i+1} = 0 \quad \forall i.$$

It has been proved in [7] 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 exponentiation.

Example. Let us illustrate the 2-NAF with the following two examples.

(1) Let us start with $n = 2^k - 1$ for some k. The binary representation is $11 \cdots 1$. But its non-adjacent form is

$$100 \cdots 0\bar{1} = 2^{k+1} - 1.$$

To get the non-adjacent form of any integer, the same process of replacing the group of 1s in the binary expansion will be used.

(2) For

$$n = (11101)_2 = 2^4 + 2^3 + 2^2 + 2^0,$$

we get

$$\text{2-NAF}(n) = (100\bar{1}01)_{\bar{2}} = 2^5 - 2^2 + 2^0.$$

(3) For

$$\begin{aligned} n &= 22453 = (101011110110101)_2 \\ &= 2^{14} + 2^{12} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^5 + 2^4 + 2^2 + 2^0, \end{aligned}$$

we get

$$\begin{aligned} \text{2-NAF}(n) &= (10\bar{1}0\bar{1}0000\bar{1}0\bar{1}0101)_{\bar{2}} \\ &= 2^{15} - 2^{13} - 2^{11} - 2^6 - 2^4 + 2^2 + 2^0. \end{aligned}$$

The addition-subtraction chain for an integer n using its non-adjacent form can be obtained by the same techniques than in the binary method. We will read the bits from left to right. There will be a doubling every time, and a $+1$ if the bit is equal to 1 and -1 if we have $\bar{1}$. Let us give some examples.

Example.

(1) Let $n = 127$. Its non-adjacent form is $1000000\bar{1}$ and the corresponding addition chain is

$$\{1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128,\ 127\}.$$

(2) Let $n = 22453$. Its non-adjacent form is $(10\bar{1}0\bar{1}0000\bar{1}0\bar{1}0101)_{\bar{2}}$ and the corresponding chain is

$$\begin{aligned} \{&1,\ 2,\ 4,\ 3,\ 6,\ 12,\ 11,\ 22,\ 44,\ 88,\ 176,\ 352,\ 351, \\ &702,\ 1404,\ 1403,\ 2806,\ 5612,\ 5613,\ 11226,\ 22452,\ 2245\}. \end{aligned}$$

1.3.3. The window method

Definition 1.8. An addition chain $\{a_0,\ a_1,\ \ldots,\ a_r\}$ is obtained using the window method of length k when it satisfies

$$\forall i \in [1, r], \exists j \in [1, i[, \text{ such that } a_i = 2a_j \text{ or } a_i = a_j + a \text{ with } a \in \mathcal{D}_k,$$

where $\mathcal{D}_k$ is a set of integers that have length k in their binary representation.

The integer k is called window length. One can remark that the binary method can be seen as a window method of length $k = 1$.

Example. Let us choose $k = 4$ and $\mathcal{D}_4 = \{5, 6, 9, 12\}$. A first chain which contains all the elements of $\mathcal{D}_3$ is $\{1, 2, 3, 5, 6, 9, 12\}$. We can then construct a window chain of length 3 for 103 as follows

$$\mathcal{C} = \{1,\ 2,\ 3,\ 5,\ 6,\ 9,\ 12, 18, 36, 41 = 36 + 5, 50 = 41 + 9, 100, 103\}.$$

2. Our use of the continued fractions

We will define the continued fractions as follows

Definition 2.1. Let n be an integer and $k \in \{2,\ 3,\ \ldots,\ n-1\}$. A 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 $b_i \in \{1, -1\}$.

We denote this generalized continued fraction expansion of $\frac{n}{k}$ by

$$[b_1 a_1,\ b_2 a_2,\ \ldots,\ b_{r-1} a_{r-1},\ a_r].$$

Example. Let $n = 927$ and $k = 365$ be, we have

$$\frac{927}{365} = 3 + \cfrac{-1}{2 + \cfrac{1}{6 + \cfrac{-1}{5 + \cfrac{-1}{6}}}},$$

$\frac{927}{365} = [-6,\ -5,\ 6,\ -2,\ 3]$.

Definition 2.2. Let $[b_1a_1,\ b_2a_2,\ \dots,\ b_{r-1}a_{r-1},\ a_r]$ be the continued fraction expansion of $\frac{n}{k}$. We define the generalized semi-continuants Q_i by:

$$Q_0 = \gcd(n,k), \qquad Q_1 = Q_0 \cdot a_1, \qquad Q_i = Q_{i-1}a_i + b_{i-1}Q_{i-2},$$
$$\forall 2 \le i \le r.$$

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

Proof. Let's prove by induction that, if $Q_o = \gcd(n,k)$, then

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

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 us 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

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

by induction, we can conclude that

$$n_0 = \frac{Q_{r-1}}{Q_0} \quad \text{and} \quad k_0 = \frac{Q_{r-2}}{Q_0},$$

and it means that

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

□

Example. Let us take a look at our previous example $\frac{927}{365} = [-6,\ -5,\ 6,\ -2,\ 3]$.

$$Q_0 = \gcd(927, 365) = 1.$$

$$Q_1 = Q_0 * a_1 = 6.$$

$$Q_2 = Q_1 * a_2 + b_1 * Q_0 = 29.$$

$$Q_3 = Q_2 * a_3 + b_2 * Q_1 = 168.$$

$$Q_4 = Q_3 * a_4 + b_3 * Q_2 = 365.$$

$$Q_5 = Q_4 * a_5 + b_4 * Q_3 = 927.$$

2.1. Computing a chain for n which contains an integer k

Let $C(d)$ be an addition-subtraction chain for $d = \gcd(n, k)$ and for $i \in [1, r]$, let $C_i = C(a_i)$ be some addition-subtraction chain for a_i, where $\frac{n}{k}$ is denoted by

$$[b_1 a_1,\ b_2 a_2,\ \ldots,\ b_{r-1} a_{r-1},\ a_r].$$

Let's define this new sequence of addition-subtraction chains X_i for all $i \in [1, r]$:

$$X_0 = C(d), \quad X_1 = X_0 \otimes C_1, \quad \text{and for all} \quad i \in [2, r].$$

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

where $\otimes$, $\oplus$ and $\ominus$ are defined as follows.

Definition 2.3.

(1)
$$c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\} \quad \text{and} \quad c_2 = \{b_0,\ b_1,\ \ldots,\ b_l\},$$
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
$$c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\} \quad \text{and} \quad m \in c_1,$$
then
$$c_1 \oplus m = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r + m\};$$

(3) if
$$c_1 = \{a_0,\ a_1,\ \ldots,\ a_r\} \quad \text{and} \quad m \in c_1,$$
then
$$c_1 \ominus m = \{a_0,\ a_1,\ \ldots,\ a_r,\ a_r - m\}.$$

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

Remark 1.

(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

$$\ell^{-}\big(C(d)\big) + r - 1 + \sum_{i=1}^{r} \ell^{-}(c_i).$$

(3) $$\ell(mn) \leq \ell(m) + \ell(n) \quad \text{and} \quad \ell^{-}(mn) \leq \ell^{-}(m) + \ell^{-}(n),$$

where ℓ^{-} stands for the minimal length of addition-subtraction chains.

Definition 2.4. 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 $\frac{n}{k}$ gives c using the method describe above.

Deciding if a given chain is a gcf-chain is difficult. We will give methods to construct good and short gcf-addition-subtraction chains for any integer n.

2.2. Our algorithm

Our algorithm MinChain $(n,\ \gamma)$ gives a gcf-chain for n using the strategy γ.

Algorithm 1: First algorithm 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, γ) is minimal
        chain = Chain(n, k, γ)
    end if
end if
Return chain
```

The following algorithm Chain(n, γ) gives the gcf-chains of n based on the minimal gcf-chains for X_i. Let us remind that X_r is a gcf-chain for n.

Algorithm 2: gcf–chain for n

Require: $n,\ k$: integers, γ: a strategy
Ensure: a sequence of integers that is a gcf-chain for n
gcf $= [u_1,\ u_2,\ \dots,\ u_r]$ the generalized continued fraction expansion of $\frac{n}{k}$
$Q_0 = \gcd(n, k)$; $Q_1 = |u_1| \cdot Q_0$;
$X_0 = \text{MinChain}(Q_0, \gamma)$; $X_1 = X_0 \otimes \text{MinChain}(|u_1|,\ \gamma)$
for $i = 0$ *to* r **do**
    $Q_i = |u_i| Q_{i-1} + \text{sign}(u_{i-1}) Q_{i-2}$
    $X_i = X_{i-1} \otimes \text{MinChain}(|u_i|,\ \gamma)$
    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

Let us take a look at an example:

EXAMPLE. $\frac{927}{365} = [-6,\ -5,\ 6,\ -2,\ 3]$.

$$C_1 = c(6) = [1,\ 2,\ 3,\ 6].$$

$$C_2 = c(5) = [1,\ 2,\ 4,\ 5].$$

$$C_3 = c(6) = [1,\ 2,\ 3,\ 6].$$

$$C_4 = C(2) = [1,\ 2].$$

$$C_5 = c(3) = [1,\ 2,\ 3].$$

Here, we obtain addition-subtraction chains X_i for all $i \in [1, 5]$.

$X_0 = [1]$.

$X_1 = X_0 \otimes C_1 = [1,\ 2,\ 3,\ 6]$.

$X_2 = X_1 \otimes C_2 \ominus Q_0 = [1,\ 2,\ 3,\ 6,\ 12,\ 24,\ 30,\ 29]$.

$X_3 = X_2 \otimes C_3 \ominus Q_1 = [1,\ 2,\ 3,\ 6,\ 12,\ 24,\ 30,\ 29,\ 58,\ 87,\ 174,\ 168]$.

$X_4 = X_3 \otimes C_4 \oplus Q_2 = [1,\ 2,\ 3,\ 6,\ 12,\ 24,\ 30,\ 29,\ 58,\ 87,\ 174,\ 168,\ 336,\ 365]$.

$X_5 = X_4 \otimes C_5 \ominus Q_3 = [1,\ 2,\ 3,\ 6,\ 12,\ 24,\ 30,\ 29,\ 58,\ 87,\ 174,\ 168,\ 336,\ 365,\ 730,\ 1095,\ 927]$.

A fast scalar multiplication for use in elliptic curve cryptography can be obtained from our method.

Example. Let E be an elliptic curve over a field of characteristic ≥ 3. Let P be a rational point of E. If we want to compute $927P$ and $365P$, we can use a gcf-addition-subtraction for 927 which contains 365. It will then be based on the continued fraction of $\frac{927}{365}$. The computation will be done as follows:

(1) Start by computing $2P,\ 3P,\ 6P$.

(2) Then, compute $12P,\ 24P,\ 30P,\ 29$.

(3) Next $58P,\ 87P,\ 174P,\ 168P$.

(4) followed by $336P,\ 365P$.

(5) Finally $730P,\ 1095P,\ 927P$.

Later, we will investigate the computation of $aP + bQ$, where P and Q are rational points of an elliptic curve.

2.3. On the strategies of choosing k

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

Definition 2.6. The floor function $\lfloor\rfloor : x \mapsto \lfloor x \rfloor$ gives the integer part of x.

Let us list some interesting strategies to compute short addition-subtraction chains.

Total Strategy:

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

Binary Strategy:

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

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

Modified-Binary Strategy:

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

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

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

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

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

Another example:

Example.

[1, 2, 4, 8, 16, 32, 64,
128, 112, 120, 240, 224, 228, 456,
448, 450, 900, 896, 1792, 1790, 3580,
3578, 7156, 7154, 7155, 14310, 14308, 28616, 28615].

Factor Strategy:

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

Pi Strategy:

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

Example.

[1, 2, 3, 6, 12, 24, 36, 42,
43, 86, 172, 344, 301, 298, 596, 894, 937].

Golden-ratio Strategy:

$$g(n) = \left\{ \left\lfloor \frac{n}{\phi} \right\rfloor \right\}.$$

with $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.

Example.

[1, 2, 4, 8, 9, 18, 27, 31, 62,
93, 84, 168, 252, 221, 442, 663, 579, 1158, 937].

Square-root Strategy:

$$\mathrm{sq}(n) = \left\{ \left\lfloor \sqrt{n} \right\rfloor \right\}.$$

Example.

[1, 2, 3, 6, 7, 10, 20, 30,
50, 51, 102, 112, 224, 275, 550, 662, 937].

Seventh Strategy:

$$\text{sevenTh}\,(n) = k,$$

where k is the greatest power of 7 less or equal to n.

Ones Strategy:

$$\text{ones}(n) = \max\{i^i,\ i^i \le n < i^{i+1} \quad \text{and} \quad \exists k \in \mathbb{N} : i = 2^k - 1\}.$$

3. Conclusion

In this paper, we have given a new method to compute short addition-subtraction chains. It is recovering most of the existing methods. Our method can be applied to design a fast scalar multiplication for use on elliptic curve cryptography. It will be further investigated to see if it resists against the Side channel attacks. The choice of k is key and we will investigate it more to see if there can be an optimal strategy.

Acknowledgment

Part of this work is done during the visit of one of the authors to the IHES (Institut de Hautes Etudes Scientifiques). The authors would like to thank the referee for the useful comments.

REFERENCES

[1] BERGERON, F.—BERSTEL, J.—BRLEK, S.—DUBOC, C.: *Addition chains using continued fractions*, J. Algorithms **10** (1989), no. 3, 403–412.

[2] BLEICHENBACHER, D.—FLAMMENKAMP, A.: *An efficient algorithm for computing shortest addition chains*, SIAM J. Discrete Math. **10** (1997), no. 1, 15–17.

[3] DOWNEY, P.—LEONG, B.—SETHI, R.: *Computing sequences with addition chains*, SIAM J. Comput. **10** (1981), no. 3, 638–646.

[4] VOLGER, H.: *Some results on addition-subtraction chains*, Inform. Process. Lett. **20** (1985), no. 3, 155–160.

[5] KNUTH, D. E.: *The Art of Computer Programming, Vol. 2. Seminumerical Algorithms.* Second edition. Addison-Wesley Series in Computer Science and Information Processing. Addison-Wesley Publishing Co., Reading, Mass., 1981.

[6] MIGNOTTE, M.—TALL, A.: *A note on addition chains*, Int. J. Algebra, **5** (2011), no. 6, 269–274.

[7] TAKAGI, T.—REIS, D.—YEN, S.—WU, B.: *Radix-r non-adjacent form and its application to pairing-based cryptosystem*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E89-A** (2006), no. 1, 115–123.
DOI: 10.1093/ietfec/e89-a.1.115

[8] TALL, A.: *A generalization of Lucas addition chains*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **55(103)** (2012), no. 1, 79–93.

[9] YACOBI, Y.: *Exponentiating faster with addition chains*, In: Advances in cryptology—EUROCRYPT '90 (Aarhus, 1990), *Lecture Notes in Comput. Sci., Vol. 473*, Springer-Verlag, Berlin, 1991. pp. 222–229,

[10] MORRAIN, F.—OLIVOS, J.: *Speeding up the computation on an elliptic curve using addition-subtraction chains*, RAIRO Informatique Théor. Appl. **24** (1990), no. 6, 531–543.

[11] GORDON, D. M.: *A survey of fast exponentiation methods* J. Algorithms 27 (1998), no. 1, 129–146.

[12] TALL, A.: *A generalization of Lucas addition chains*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **55 (103)** (2012), 79–93.

Received December 3, 2022

Moussa Ngom
Amadou Tall
Departement de Mathématiques et Informatique
Faculté des Sciences et Techniques
Université Cheikh Anta Diop de Dakar
SENEGAL

E-mail: moussa8.ngom@ucad.edu.sn
amadou7.tall@ucad.edu.sn