Math-for-industry
Education & Research Hub

On the zero-run length of a signed binary representation

Hisashi Yamada, Tsuyoshi Takagi and Kouichi Sakurai

Received on February 22, 2009

Abstract. Elliptic curve cryptosystems (ECC) are suitable for memory-constraint devices like smart cards due to their small key-size. Non-adjacent form (NAF) is a signed binary representation of integers used for implementing ECC. Recently, Schmidt-Samoa et al. proposed the fractional wMOF (Frac-wMOF), which is a left-to-right analogue of NAF, where w is the fractional window size $w = w_0 + w_1$ of integer w_0 and fractional number w_1. On the contrary to NAF, there are some consecutive none-zero bits in Frac-wMOF, and thus the zero-run length of the Frac-wMOF is not equal to that of the variants of NAF. In this paper we present an asymptotic formula of zero-run length of Frac-wMOF. Indeed, the average zero-run length of the Frac-wMOF is asymptotically $w\frac{2^{w_0+1}}{2^{w_0+1}-1}$, which is longer than that of the fractional wNAF.

Keywords. elliptic curve cryptosystem, signed binary representations, zero-run length.

1. Introduction

One of the research topics in elliptic curve cryptosystems is how to enhance the speed of computing scalar multiplication dP, where d is an integer and P is a point on the elliptic curve. We deal with the representation problem of integer

$$d = \sum_{i=0}^{n-1} d_i 2^i = (d_{n-1}, d_{n-2}, ..., d_0), d_i \in T$$

for a given digit set T and some integer n. Here the binary representation of d chooses $T = \{0, 1\}$, but d can be represented in many different ways if the digit set T is allowed to have redundancy, e.g. $T = \{0, \pm 1\}$. An efficient scalar multiplication can be achieved by the representation of integer d with a small Hamming weight (the number of $d_i \neq 0$) and a small digit set T.

The most popular class in the redundant representations is Non-Adjacent Form (NAF) [10]. NAF is uniquely defined by the property of $d_i d_{i+1} = 0$ and $d_i \in \{0, \pm 1\}$ for any integer i. It is known that NAF have the minimal Hamming weight in the redundant representations of $T \in \{0, \pm 1\}$ and the average density of non-zero digits in NAF is $\frac{1}{3}$. Therefore, NAF is more efficient class than the binary representation for ECC. Next wNAF is an extension of NAF with the redundant digit set $T_w = \{0, \pm 1, \pm 3, ..., \pm(2^{w-1} - 1)\}$ of d, which has at most one non-zero digit among w consecutive digits [10]. wNAF has the minimal Hamming weight in the redundant representations of the digit set T_w, and the average density of non-zero digits in wNAF is $\frac{1}{1+w}$. Moreover, the window size w can be extended to the fractional window size $w = w_0 + w_1$, where w_0 is an integer and w_1 is a fractional number. Fractional wNAF (Frac-wNAF) uses the redundant digit set $T_{w_0+w_1} = \{0, \pm 1, \pm 3, ..., \pm(2^{w_0-1} - 1), \pm(2^{w_0-1} + 1), ..., \pm((1 + w_1)2^{w_0-1} - 1)\}$ of d, and thus size of the digit set is flexibly chosen [7]. It is known that Frac-wNAF has the minimal hamming weight in the redundant representations of the given digit set $T_{w_0+w_1}$ and the average density of non-zero digits in Frac-wNAF is $\frac{1}{1+w_0+w_1} = \frac{1}{1+w}$. This method gives the most suitable solution for the afore-mentioned problem.

On the other hand, the scalar multiplication is usually computed from the most digit (left-to-right), but (Frac-)wNAF is generated from the binary representation starting with the lower digit (right-to-left) maintaining a propagation digit. Therefore (Frac-)wNAF is not most suitable for the implementation on a memory-constrained device. Okeya *et al.* proposed the width-w Mutual Opposite Form (MOF), which is a left-to-right analogue of wNAF, and wMOF has the minimal Hamming weight same as wNAF [8]. Moreover, Schmidt-Samoa *et al.* proposed Frac-wMOF which applies the fractional window method to wMOF [9]. Frac-wMOF is the most suitable method for the implementation of ECC.

1.1. Our Contributions

In this paper, we analyze the distribution of non-zero digits of Frac-wMOF. On the contrary to Frac-wNAF, some consecutive non-zero digits appear in Frac-wMOF. The consecutive non-zero digits make the average zero-run length of Frac-wMOF longer than that of Frac-wNAF, namely $w = w_0 + w_1$. We try to estimate the asymptotic distribution of the digits appeared in Frac-wMOF. At first the presentation of Frac-wMOF is decomposed into several syntax blocks based on the conversion table of Frac-wMOF. We prove that the blocks are related with an irreducible and aperiodic transit matrix of Markov chain. From the stationary distribution of the transit matrix we estimate the distribution of the consecutive non-zero digits of Frac-wMOF. Finally we prove the average zero-run of Frac-wMOF is asymptotically $w\frac{2^{w_0+1}}{2^{w_0+1}-1}$. We also present some experimental data that evaluate this theoretical estimation.

The organization of this paper is as follows: In Section 2, we describe the generation algorithm and some mathematical properties related to Frac-wMOF. In Section 3, we estimate the density of the consecutive non-zero digits and the zero-run length of Frac-wMOF. We also present some experimental results of our zero-run length formula. In Section 4, we state some concluding remarks.

2. Frac-wMOF

In this section, we review the definition and generation method of Frac-wMOF, which is an analogue of Frac-wNAF.

2.1. wNAF, wMOF

Each positive integer can be uniquely represented by Booth encoding. The Booth encoding of an integer d is an signed binary representation $d = \sum_{i=0}^{n} \beta_i 2^i, \beta_i \in T, T = \{0, \pm 1\}$ and $B(d) = (\beta_n, \beta_{n-1}, ..., \beta_0)$, which is obtained by the bitwise subtraction $B(d) = 2d \ominus d$ [2]. It is easy to see that the average density of non-zero digit is asymptotically 1/2. Here the Booth encoding of an integer d satisfies the following two properties:

- the signs of adjacent non-zero digits (without considering 0 bits) are opposite.
- the most non-zero digit and the least non-zero digit are 1 and -1 (we describe -1 as $\bar{1}$ from now on), respectively, unless all digits are zero.

Okeya *et al.* showed that wNAF can be generated by applying the window method with the window size w to the Booth encoding in right-to-left [8]. On the other hand, wMOF is a dual class of wNAF, which is defined as the representation which applies the window method with the window size w to the Booth encoding in left-to-right. Here the window method with the window size w is a method that converts the consecutive w digits starting with the non-zero digit into $(w-1)$ zero digits with one integer value after scanning the Booth encoding one digit by one digit (we skip to the next digit if the zero digit is scanned). Denote by $\mathit{Table}[w]$ the conversion table for generating wMOF. We present the conversion tables for $w = 3$ and $w = 4$ as follows.

The conversion table $\mathit{Table}[3]$ for window size 3

$100 \to 100$	$1\bar{1}0 \to 010$	$1\bar{1}1 \to 003$	$\bar{1}1\bar{1} \to 00\bar{3}$
$\bar{1}00 \to \bar{1}00$	$\bar{1}10 \to 0\bar{1}0$	$10\bar{1} \to 003$	$\bar{1}01 \to 00\bar{3}$

The conversion table $\mathit{Table}[4]$ for window size 4

$1000 \to 1000$	$1\bar{1}10 \to 0030$	$1\bar{1}01 \to 0005$	$100\bar{1} \to 0007$
$\bar{1}000 \to \bar{1}000$	$10\bar{1}0 \to 0030$	$1\bar{1}1\bar{1} \to 0005$	$10\bar{1}1 \to 0007$
$1\bar{1}00 \to 0100$	$\bar{1}1\bar{1}0 \to 00\bar{3}0$	$\bar{1}10\bar{1} \to 000\bar{5}$	$\bar{1}001 \to 000\bar{7}$
$\bar{1}100 \to 0\bar{1}00$	$\bar{1}010 \to 00\bar{3}0$	$\bar{1}1\bar{1}1 \to 000\bar{5}$	$\bar{1}01\bar{1} \to 000\bar{7}$

The number of an element in $\mathit{Table}[w]$ is 2^w. Here the non-zero digit after the conversion appears in the lowest digit (the right-side edge) or the highest digit (the left-side edge) in the consecutive w digits. Therefore wMOF has the consecutive non-zero digits (*e.g.* $|0007|1000|$ in the above table). Note that the length of the consecutive non-zero digits is not longer than two. On the other hand, wNAF is generated with a conversion table starting with the lower non-zero digit (left-to-right). wNAF thus has no consecutive non-zero digits, because a non-zero digit only appears in the lowest digit (the right-side edge). The average zero-run length of wNAF is obviously w. It is known that the Hamming weight of wMOF is equal to that of wNAF, which is the minimal in the redundant representation of the digit set $\{0, \pm 1, \pm 3, ..., \pm(2^{w-1}-1)\}$. The average density of non-zero digits of both wMOF and wNAF is asymptotically $\frac{1}{1+w}$ [8].

2.2. Frac-wMOF

The wMOF utilizes the redundant digit set $T_w = \{0, \pm 1, \pm 3, ..., \pm(2^{w-1}-1)\}$ defined for natural number w. A scalar multiplication by wMOF should pre-compute the points $P_{2j+1} = (2j+1)P$ for $0 \leq j \leq 2^{w-1}-1$, namely we store 2^{w-2} points in memory. Therefore the memory size for the pre-computation increases exponentially in w and their size takes only the discrete values. It is not suitable for memory-constraint devices. For example, we assume a device which can only store 3 pre-computed points. The number of the non-zero digits for $w = 3$ is $2^{3-2} = 2$, and thus the memory space for one more point is free. However we cannot choose the window size $w = 4$, which needs $2^{4-2} = 4$ points for the pre-computation.

Fractional wMOF can solve the problem successfully [9]. Now, for any positive integer q we try to construct the digit set $\{0, \pm 1, \pm 3, ..., \pm(2q-1)\}$ with q elements. Let w_0 be an integer which satisfies $2^{w_0-2} \leq q < 2^{w_0-1}$, and let w_1 be a fractional number $w_1 = \frac{q-2^{w_0-2}}{2^{w_0-2}}$. Here we define the window size w of Frac-wMOF as $w = w_0 + w_1$. This fractional number w_1 is in the interval $0 \leq w_1 < 1$, and the window size which becomes an integer. The digit set of Frac-wMOF with the window size $w = w_0 + w_1$ is equal to $T_{w_0+w_1} = \{0, \pm 1, \pm 3, ..., \pm(2^{w_0-1}-1), \pm(2^{w_0-1}+1), ..., \pm((1+w_1)2^{w_0-1}-1)\}$, and the number of the non-zero digits in $T_{w_0+w_1}$ is $q = (1+w_1)2^{w_0-2}$ for the window size w.

The conversion table of Frac-wMOF with the window size $w = w_0 + w_1$ consists of two tables with an integer window size, namely w_0 and w_0+1. If the consecutive (w_0+1) digits starting with the non-zero digit are contained in digit set $T_{w_0+w_1}$ as integer, then the conversion table for the window size w_0+1 is used. Otherwise we should switch to the conversion table for the window size w_0. The number of elements in the conversion table of Frac-wMOF is either $(1+w_1)2^{w_0}$ for the window size w_0+1 or $(1-w_1)2^{w_0}$ for the window size w_0. For example, the number of the non-zero digit for the window size $w = 3\frac{1}{2}$ is $(1+\frac{1}{2})2^{3-2} = 3$, and their conversion table is as follows:

The conversion table *Table*$[3\frac{1}{2}]$ for window size $3\frac{1}{2}$

$1000 \rightarrow 1000$	$1\bar{1}10 \rightarrow 0030$	$1\bar{1}01 \rightarrow 0005$	$100 \rightarrow 100$
$\bar{1}000 \rightarrow \bar{1}000$	$10\bar{1}0 \rightarrow 0030$	$1\bar{1}1\bar{1} \rightarrow 0005$	$10\bar{1} \rightarrow 003$
$1\bar{1}00 \rightarrow 0100$	$\bar{1}1\bar{1}0 \rightarrow 00\bar{3}0$	$\bar{1}10\bar{1} \rightarrow 000\bar{5}$	$\bar{1}00 \rightarrow \bar{1}00$
$\bar{1}100 \rightarrow 0\bar{1}00$	$\bar{1}010 \rightarrow 00\bar{3}0$	$\bar{1}1\bar{1}1 \rightarrow 000\bar{5}$	$\bar{1}01 \rightarrow 00\bar{3}$

Here we present an algorithm which generates Frac-wMOF from a binary representation d.

Algorithm 1: Generation of Frac-wMOF [9]

```
Input: binary representation $d = (d_{n-1}, d_{n-2}, ..., d_0)$,
       the window size $w = w_0 + w_1$,
Output: Frac-$w$MOF $d = (\mu_n, \mu_{n-1}, ..., \mu_0)$.
1: $B(d) \leftarrow 2d \ominus d$, $i \leftarrow n$, $\beta_{-1} \leftarrow 0, \dots, \beta_{-w+1} \leftarrow 0$;
2: while $i \geq 0$ do
3:   if $\beta_i = 0$ then $\mu_i \leftarrow 0, i \leftarrow i-1$ else do
4:   if $|\sum_{j=1}^{w_0+1} \beta_{i+j-w_0-1} 2^{j-1}| \geq 2^{w_0-1}(1+w_1)$
5:   then $(\mu_i, ..., \mu_{i-w_0+1}) \leftarrow Table[w_0](\beta_i, ..., \beta_{i-w_0+1})$,
         $i \leftarrow i - w_0$;
6:   else $(\mu_i, ..., \mu_{i-w_0}) \leftarrow Table[w_0+1](\beta_i, ..., \beta_{i-w_0})$,
         $i \leftarrow i - w_0 - 1$;
7: Return $(\mu_n, \mu_{n-1}, ..., \mu_0)$
```

In step 1, we compute the Booth encoding $B(d)$ of integer d and initialize some values. From step 2 to 6, we compute the main loop in terms of scanning the digit β_i for $i = n, n-1, ..., 1, 0$. If i-th digit β_i is zero, we assign $\mu_i = 0$ and skip to the lower digit. Otherwise we scan (w_0+1) consecutive digits $(\beta_i, \beta_{i-1}, ..., \beta_{i-w_0})$ and check if or not $W = \sum_{j=1}^{w_0+1} \beta_{i+j-w_0-1} 2^{j-1}$ in the conversion table of Frac-wMOF, namely $|W| \geq 2^{w_0-1}(1+w_1)$ in step 4. When W is not contained in the conversion table, we convert w_0 consecutive digits $(\beta_i, \beta_{i-1}, ..., \beta_{i-w_0+1})$ using the conversion table *Table*$[w_0]$ in step 5. Otherwise (w_0+1) consecutive digits $(\beta_i, \beta_{i-1}, ..., \beta_{i-w_0})$ are converted by *Table*$[w_0+1]$ in step 6.

Frac-wMOF representation of integer d is a class which has the minimal Hamming weight in the digit set $T_{w_0+w_1}$. Denote by $H(n)$ and $L(n)$ the average number of non-zero digits and the average length for integers at most n bits, respectively. It is known that $H(n) = \frac{1}{1+w_0+w_1}n + c_H + \mathcal{O}(2^{-n})$ and $L(n) = n + c_L + \mathcal{O}(2^{-n})$, where c_H, c_L are some constants [9].

2.3. Blocks in Frac-wMOF

We discuss the average length of the consecutive non-zero digits in Frac-wMOF.

From Algorithm 1 we define the following blocks appeared in Frac-wMOF

$$\underbrace{0}_{1}, \underbrace{0..*..0}_{w_0}, \underbrace{0...*...0}_{w_0+1},$$

where $*$ is the non-zero digit in the digit set $T_{w_0+w_1}$. The above three blocks are denoted by I, II, and III, respectively. The digits of Frac-wMOF is composed by one of the syntax blocks I, II, and III. Block I is $\mu_i = 0$ in step 3 of Algorithm 1, which is generated for $\beta_i = 0$. If $\beta_i \neq 0$ holds, then either II in step 5 or III in step 6 is generated instead of I. Let $(1-R), R$ be the appearance probability of blocks II, III, respectively. This probability depends only on the window size $w = w_0 + w_1$. In this paper we deal with the asymptotic behavior of blocks I, II, and III for enough large n of input $d = (d_{n-1}, d_{n-2}..., d_0)$ in Algorithm 1. Let Q_1, Q_2, Q_3 be the asymptotic appearance probabilities of the above each block I, II, III.

The appearance probability R of the block III in Algorithm 1 can be estimated in the following. In step 5 and 6 of Algorithm 1 we use the conversion table *Table*$[w_0]$ and *Table*$[w_0+1]$, respectively. The choice of the conversion tables depends on the (w_0+1) consecutive digits $(\beta_i, \beta_{i-1}, ..., \beta_{i-w_0})$ in step 4, and some elements in each conversion table are never used. The appearance probability R is estimated by the number used in each conversion table. At first note that there are 2^{w_0+1} possible elements in step 4. Step 6 is processed if $|W| < 2^{w_0-1}(1+w_1)$ holds in step 4, where $W = \sum_{j=1}^{w_0+1} \beta_{i+j-w_0-1} 2^{j-1}$. Therefore we use $2^{w_0} + w_1 2^{w_0}$ elements in the conversion table *Table*$[w_0+1]$ in step 6 of Algorithm 1, Consequently, the appearance probability is $R = \frac{2^{w_0} + w_1 2^{w_0}}{2^{w_0+1}} = \frac{1+w_1}{2}$ from above consideration.

2.4. Stationary Distribution of Blocks

The stationary distribution of the syntax blocks Q_1, Q_2, Q_3 of Frac-wMOF can be estimated by the same way appeared in [9].

At first we try to construct a transition matrix of the syntax blocks I, II or III. If the current state is the block I, the lower block is either I, II or III. There is no propagation digit among the blocks. The appearance probability of the block I after I is equal to $\frac{1}{2}$, which is the probability that the highest digit in the block I is zero. The probability that II or III appears after I is $\frac{1}{2}(1-R)$ or $\frac{1}{2}R$, respectively. Next, recall that the block II appears if $|W| \geq 2^{w_0-1}(1+w_1)$ holds in step 4, where $W = \sum_{j=1}^{w_0+1} \beta_{i+j-w_0-1} 2^{j-1}$. Therefore the lowest digit β_{i-w_0-1} of the consecutive (w_0+1) digits that will be converted to II is always non-zero. It means that the lower block after II is only either the block II or III. Therefore, the probability that the lower block after II becomes III or II is R or $1-R$, respectively. The appearance probability of the blocks after III can be estimated in a similar way of the case for I. The probability that the lower block of III becomes I, II, and III is $\frac{1}{2}$, $\frac{1}{2}R$, and $\frac{1}{2}(1-R)$, respectively.

From the above discussion, we have obtained the transition matrix of the syntax blocks I, II, III, which is the following 3×3 matrix.

	I	II	III
I	$\frac{1}{2}$	$\frac{1}{2}(1-R)$	$\frac{1}{2}R$
II	0	$1-R$	R
III	$\frac{1}{2}$	$\frac{1}{2}(1-R)$	$\frac{1}{2}R$

As $0 < w_1 < 1$ holds, this Markov chain is irreducible and aperiodic, and thus its stationary distribution can be determined as

$$\begin{aligned}(Q_1,\, Q_2,\, Q_3) &= \left(\frac{R}{R+1}, \frac{1-R}{R+1}, \frac{R}{R+1}\right) \\ &= \left(\frac{1+w_1}{3+w_1}, \frac{1-w_1}{3+w_1}, \frac{1+w_1}{3+w_1}\right).\end{aligned}$$

The convergence speed to the stationary distributions Q_1, Q_2, Q_3 is $\mathcal{O}(2^{-n})$, where n is the bit length of the input integer in Algorithm 1.

If $w_1 = 0$, we can discuss the stationary distribution of the syntax blocks of wMOF from similar above consideration.

3. Zero-Run Length in Frac-wMOF

In this section, we discuss the average length of the consecutive non-zero digits in Frac-wMOF, and then we estimate the average zero-run length in Frac-wMOF.

3.1. Zero-Run Length

We defined the notations used in this paper in the following. Let d be an integer d at most n bits (*i.e.* $d = 0, 1, 2, ..., 2^n - 1$), and let $M(d) = \sum_{i=0}^{n} \mu_i 2^i = (\mu_n, \mu_{n-1}, ..., \mu_0)$ be the Frac-wMOF of integer d with width w. We call d_i the i-th digit of μ, and the zero digit is a digit of $\mu_i = 0$ for $i = 0, 1, 2, ..., n$. The Hamming weight of $M(d)$, which is denoted by $h(M(d))$, is the total number of the non-zero digits of μ_i, namely $h(M(d)) = \#\{\mu_i \neq 0 | M(d) = (\mu_n, \mu_{n-1}, ..., \mu_0)\}$. Let $l(M(d))$ be the digit length of $M(d)$ which is the largest i with $\mu_i \neq 0$ among $i = 0, 1, 2, ..., n$ for $d \neq 0$ (we define $l(M(0)) = 0$). Recall that the length of the consecutive non-zero digits of Frac-wMOF is not longer than two. The consecutive non-zero digits have the form $0, \mu_j, \mu_{j-1}, 0$, where both $\mu_j \neq 0$ and $\mu_{j-1} \neq 0$ for some j. Denote by Let $c(M(d))$ be the number of the consecutive non-zero digits appeared in $M(d)$. The zero-run length $zr(M(d))$ of $M(d)$ is defined by

$$zr(M(d)) = \begin{cases} \dfrac{l(M(d)) - h(M(d))}{h(M(d)) - c(M(d)) - 1} & \text{(if } d \text{ is odd)} \\[2ex] \dfrac{l(M(d)) - h(M(d))}{h(M(d)) - c(M(d))} & \text{(if } d \text{ is even)} \end{cases}$$

Next we define the average number of non-zero digits $H(n)$, the average digit length $L(n)$, and the average number of the consecutive non-zero $C_T(n)$ for Frac-wMOF of all integers at most n bits as follows:

$$\begin{aligned} H(n) &= \frac{\sum_{d=0}^{2^n-1} h(M(d))}{2^n}, \\ L(n) &= \frac{\sum_{d=0}^{2^n-1} l(M(d))}{2^n}, \\ C(n) &= \frac{\sum_{d=0}^{2^n-1} c(M(d))}{2^n}. \end{aligned}$$

Finally, the average zero-run length $ZR(n)$ for Frac-wMOF of all integers at most n bits is defined by

$$(1) \qquad ZR(n) = \frac{L(n)2^n - H(n)2^n}{H(n)2^n - 2^{n-1} - C(n)2^n}.$$

3.2. The Detailed Probability of Each Block

We consider the case that the lowest digit (or the highest digit) of bocks II, III becomes the non-zero digit $* \in T_w$. Denote by $Q_2^{(r)}$ (or $Q_2^{(l)}$) the probability of $(0...0*)$ (or $(*0...0)$) in the block II. Denote by $Q_3^{(r)}$ (or $Q_3^{(l)}$) the probability of $(0...0*)$ (or $(*0...0)$) in the block III. These notations are used for the estimating density of the consecutive non-zero digits in Frac-wMOF.

We estimate the probabilities $Q_2^{(l)}, Q_2^{(r)}, Q_3^{(l)}, Q_3^{(r)}$ that the lowest or highest bit in the blocks II, III becomes a non-zero digit. Let $*$ be the non-zero digit in the digit set T_w. We consider the probability that the pattern $(0...0*)$ appears in the block II. After converting the consecutive w_0 digits $(\beta_i, \beta_{i-1}, ..., \beta_{i-w_0+1})$ in Algorithm 1, the lowest digit becomes a non-zero digit with probability $\frac{1}{2}$. The pattern $(0...0*)$ appears if the lowest digit is a non-zero digit, and thus $Q_2^{(r)} = \frac{(1-w_1 2^{w_0-1})}{(1-w_1)2^{w_0}} = \frac{1}{2}$. Here, the pattern $(*0...0)$ appeared in the block III is only either $(10...0)$ or $(\bar{1}0...0)$. The total number of elements in the block II is $2^{w_0+1} - (1+w_1)2^{w_0} = (1+w_1)2^{w_0}$. Therefore, we obtain $Q_2^{(l)} = \frac{1}{(1-w_1)2^{w_0-1}}$.

The number of the pattern $(0...0*)$ appeared in the block III is equal to $\frac{2^{w_0+1}}{2} - (1-w_1)2^{w_0} = w_1 2^{w_0}$, where $\frac{2^{w_0+1}}{2}$ is the half of 2^{w_0+1} possible elements in step 4 of Algorithm 1 and $(1-w_1)2^{w_0}$ is the total number in the block III. Therefore, the conditional probability $Q_3^{(r)}$ is $\frac{w_1 2^{w_0}}{(1+w_1)2^{w_0}} = \frac{w_1}{1+w_1}$. There are only two elements whose pattern in the block II becomes $(0...0*)$ as we discussed in the case of the block III. Therefore, the conditional probability is $Q_3^{(l)} = \frac{2}{(1+w_1)2^{w_0}} = \frac{1}{(1+w_1)2^{w_0-1}}$.

3.3. Distribution of Consecutive Non-Zero Digits

We analyze the average number of consecutive non-zero digits appeared in Frac-wMOF in the following.

Theorem 1. *The average number of consecutive non-zero digits in Frac-wMOF converted from integers at most n bit* *is*

$$C(n) = \frac{1}{(1+w)2^{w_0+1}} n + c_C + \mathcal{O}(2^{-n})$$

for the window size $w = w_0 + w_1$ and some constant c_C.

Proof. At first the stationary distribution and the length of three blocks I, II, III is Q_1, Q_2, Q_3 and $1, w_0, (w_0+1)$, respectively. Therefore the average length of the above three blocks appeared in Frac-wMOF is

$$X = Q_1 + w_0 Q_2 + (w_0+1)Q_3 = \frac{2(1+w)}{3+w_1}.$$

Next we estimate the average length of the consecutive non-zero digits in the three blocks, which is denoted by Y. The consecutive non-zero digits are only the following 4 patterns.

$$|\underbrace{(0...0*)}_{w_0+1}|\underbrace{(*0...0)}_{w_0+1}|, \quad |\underbrace{(0...0*)}_{w_0+1}|\underbrace{(*0..0)}_{w_0}|,$$
$$|\underbrace{(0..0*)}_{w_0}|\underbrace{(*0...0)}_{w_0+1}|, \quad |\underbrace{(0..0*)}_{w_0}|\underbrace{(*0..0)}_{w_0}|,$$

where $*$ is one of the non-zero digits in digit set T_w. Therefore Y can be estimated by the probabilities $Q_2^{(r)}$, $Q_2^{(l)}$, $Q_3^{(r)}$, $Q_3^{(l)}$ in the previous section, namely we have

$$\begin{aligned} Y &= Q_3 Q_3^{(r)} \left\{ \frac{1}{2} R Q_3^{(l)} + \frac{1}{2}(1-R) Q_2^{(l)} \right\} \\ &\quad + Q_2 Q_2^{(r)} \left\{ R Q_3^{(l)} + (1-R) Q_2^{(l)} \right\} \\ &= \frac{1}{(3+w_1)2^{w_0}}. \end{aligned}$$

In this paper we assume that Frac-wMOF is converted from integers at most n bits and the average estimation is calculated over all integers at most n bits. The average lengths X and Y are converged in the speed $\mathcal{O}(2^{-n})$ because of the stationary distributions Q_1, Q_2, Q_3. Therefore the average density of the consecutive non-zero digits can be estimated by

$$\frac{Y}{X} = \frac{1}{(3+w_1)2^{w_0}} \frac{3+w_1}{2(1+w)} = \frac{1}{(1+w)2^{w_0+1}}.$$

From the above facts, the average number of the consecutive non-zero digits in Frac-wMOF converted from integers at most n bits is $C(n) = \frac{1}{(1+w)2^{w_0+1}} n + c_C + \mathcal{O}(2^{-n})$ for some constant c_C. □

3.4. Average Zero-Run Length in Frac-wMOF

We can prove the following theorem from the discussion in the previous sections.

Theorem 2. *The average zero-run length of Frac-wMOF converted from integers at most n bits is*

$$w \frac{2^{w_0+1}}{2^{w_0+1}-1} + \mathcal{O}(n^{-1})$$

for the window size $w = w_0 + w_1$.

Proof. Denote by $ZR(n)$ the average zero-run length of Frac-wMOF converted from integers at most n bits. From the definition in Section 3, we are able to evaluate $ZR(n)$ by the following formula. $ZR(n) = \frac{L(n)2^n - H(n)2^n}{H(n)2^n - 2^{n-1} - C(n)2^n}$, where $L(n) = n + c_L + \mathcal{O}(2^{-n})$, $H(n) = \frac{1}{1+w} n + c_L + \mathcal{O}(2^{-n})$, and $C(n) = \frac{1}{(1+w)2^{w_0+1}} n + c_C + \mathcal{O}(2^{-n})$ appeared in Theorem 1. By dividing this equation by $n2^n$ we obtain

$$ZR(n) = \frac{\frac{L(n)}{n} - \frac{H(n)}{n}}{\frac{H(n)}{n} - \frac{C(n)}{n} - \frac{1}{2n}}.$$

Therefore, the average zero-run length of Frac-wMOF with window size $w = w_0 + w_1$ is equal to

$$ZR(n) = w \frac{2^{w_0+1}}{2^{w_0+1}-1} + \mathcal{O}(n^{-1}).$$

□

In the case of $w = 2$, Han *et al.* proved the average zero-run length of 2MOF converted from integer at most n bits is $\frac{16}{7}$ for $n \to \infty$ [5]. The zero-run formula in Theorem 2 is a natural extension of their result.

3.5. Comparison

We compare Frac-wNAF with Frac-wMOF in the following. Table 1 describes the average density of the non-zero digits (Non-Zero Density) and the zero-run length (Zero-Run) of both Frac-wNAF and Frac-wMOF.

Table 1: Comparison of Frac-wMOF with Frac-wNAF

Scheme	Non-Zero Density [9]	Zero-Run Length
Frac-wNAF	$\frac{1}{1+w_0+w_1}$	$w_0 + w_1$
Frac-wMOF	$\frac{1}{1+w_0+w_1}$	$(w_0 + w_1)\frac{2^{w_0+1}}{2^{w_0+1}-1}$

The average density of non-zero in Frac-wMOF is equal to that of Frac-wNAF [9], but their average zero-run length is different due to the consecutive non-zero digits appeared in Frac-wMOF. Indeed, the average zero-run length in Frac-wMOF is $\frac{2^{w_0+1}}{2^{w_0+1}-1}$ times longer than that in Frac-wNAF. For example, when we assume $w = 3\frac{1}{2}$, the average zero-run length in Frac-$3\frac{1}{2}$MOF is $\frac{56}{15}$, that value is longer than $\frac{7}{2}$ which is the average zero-run length in Frac-$3\frac{1}{2}$NAF.

3.6. Experiment Results

In order to evaluate the formula of the zero-run length of Frac-wMOF in the previous section, we present some experimental data for random inputs of the fixed bit lengths and several window size $w = w_0 + w_1$.

The zero-run formula in Theorem 2 aims at evaluating the asymptotic behavior of Frac-wMOF for integers at most n bits. Therefore, the first experiment chooses an enough large length $n = 1,000,000$, in which we count the average zero-run of Frac-wMOF converted from a randomly chosen integer of one million bits. Next the practical key length of elliptic curve cryptosystems is usually chosen larger than

160 bits, and the scalar multiplication deploys many different ephemeral random integers. Therefore, the second experiment chooses $n = 160$ and evaluated the average zero-run length for one million randomly integers. In Table 2 we present the experimental results.

Table 2: Experiment Results

w	Theoretical Values	Experimental Values	
		1 million bits	160 bits
2	2.286	2.286	2.265
3	3.200	3.200	3.143
$3\frac{1}{2}$	3.733	3.733	3.654
4	4.129	4.129	4.009
$4\frac{1}{4}$	4.387	4.387	4.252
$4\frac{1}{2}$	4.645	4.645	4.494
$4\frac{3}{4}$	4.903	4.903	4.734
5	5.079	5.080	4.863
$5\frac{1}{8}$	5.206	5.204	4.979
$5\frac{1}{4}$	5.333	5.335	5.096
$5\frac{3}{8}$	5.460	5.460	5.212
$5\frac{1}{2}$	5.587	5.587	5.329
$5\frac{5}{8}$	5.714	5.716	5.444
$5\frac{3}{4}$	5.841	5.840	5.560
$5\frac{7}{8}$	5.968	5.975	5.675
6	6.047	6.050	5.693

The experimental values for $n = 1,000,000$ coincide with the theoretical ones with the error rates under 0.12%. On the other hand, the experimental values for $n = 160$ differ from the theoretical ones with the error rates about several percents. This differences arise from the convergence speed $\mathcal{O}(n^{-1})$ of the zero-run formula in Theorem 2.

4. Conclusion

In this paper, we presented an asymptotic formula of zero-run length of Frac-wMOF, which is a left-to-right analogue of Frac-wNAF. We classified the chain of Frac-wMOF into several syntax blocks and evaluated their asymptotic distributions using the Markov chain. The average zero-run length of Frac-wMOF converted from integers at most n bits is $w\frac{2^{w_0+1}}{2^{w_0+1}-1}$ for window size $w = w_0 + w_1$ and $n \to \infty$. We also showed some experimental results for Frac-wMOF of one million digits and 160 bits.

References

[1] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptogracphy*, Cambridge University, 1999

[2] A. Booth, "A Signed Binary Multiplication Technique", Quarterly Journal of Mechanics and Applied Mathematics, Vol.4, No.2, pp.236-240, 1951.

[3] H. Cohen, "Analysis of the Sliding Window Powering Algorithm", Journal of Cryptology, Vol.18, No.1, pp.63-76, 2005.

[4] H. Cohen, A. Miyaji, and T. Ono, "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates", ASIACRYPT'98, LNCS 1514, pp.51-65, 1998.

[5] D. -G. Han, T. Izu, and T. Takagi, "Some Explicit Formulae of NAF and its Left-to-Right Analogue", Cryptology ePrint Archive 2005/384, 2005.

[6] M. Joye, and S.-M. Yen, "Optimal Left-to-right Binary Signed-Digit Recording", IEEE Transactions on Computers, Vol.49, No.7, pp.740-748, 2000.

[7] B. Möller, "Improved Techniques for Fast Exponentiation", ICISC 2003, LNCS 2587, pp.298-312, 2003.

[8] K. Okeya, K. Schmidt-Smoa, C. Spahn, and T. Takagi, "Signed Binary Representations Revisited", CRYPTO 2004, LNCS 3152, pp.123-139, 2004.

[9] K. Schmidt-Samoa, O. Semay, and T .Takagi, "Analysis of Fractional Window Recoding Methods and Their Application to Elliptic Curve Cryptosystems", IEEE Transactions on Computers, Vol.55, No.1, pp.48-57, 2006.

[10] J. Solinas, "Efficient Arithmetic on Koblitz Curves", Designs, Codes, and Cryptography, Vol.19, No.2-3, pp.195-249, 2000.

Contact Address:

Hisashi Yamada,
Graduate School of Systems Information Science, Future University Hakodate, 041-8655, Japan.

Tsuyoshi Takagi
Graduate School of Systems Information Science, Future University Hakodate, 041-8655, Japan.
E-mail: takagi(at)fun.ac.jp

Kouichi Sakurai
Graduate School of Information Science and Electrical Engineering, Kyushu University, 819-0395, Japan.
E-mail: sakurai(at)csce.kyushu-u.ac.jp