JSIAM Letters Vol.9 (2017) pp.5–8 ©2017 Japan Society for Industrial and Applied Mathematics

One-stroke polynomials over a ring of modulo 2^w

Atsushi Iwasaki[1] and Ken Umeno[1]

[1] Graduate school of Informatics, Kyoto University, Yoshida-honmachi, Kyoto, Japan

E-mail *iwasaki.atsushi.47e@kyoto-u.jp, umeno.ken.8z@kyoto-u.ac.jp*

Received May 29, 2016, Accepted November 19, 2016

Abstract

Permutation polynomials over a ring of modulo 2^w are well adopted to digital computers and digital signal processors, and so they are in particular expected to be useful for cryptography and pseudo random number generators. For a longer period of the polynomial is demanded in general, we derive a necessary and sufficient condition that polynomials are permutating and their periods are the longest over the ring. We call polynomials which satisfy the condition "one-stroke polynomials over the ring".

Keywords permutation polynomial, modulo 2^w, cryptography, pseudo random number generator

Research Activity Group Applied Chaos

1. Introduction

A polynomial is called a permutation polynomial over a finite ring R if the polynomial is bijection over R. Although R is a finite field in many studies, we deal with a ring of modulo 2^w in this paper. Studies about permutation polynomials over the ring are very important because they are well adopted to with digital computers and digital signal processors. They can calculate values of permutation polynomials over the ring faster than over a finite field because 2 power residue operation is practically negligible. Then, they are in particular expected to be useful for cryptography and pseudo random number generators, and some applications have been already proposed [1–3].

There are two important studies about permutation polynomials over the ring. One is about periods of the polynomials. For cryptography and pseudo random number generators, such periods are expected to be longer. Then, a necessary and sufficient condition to maximize the periods of the permutation polynomials should be explored. When the period of the permutation polynomial is maximized, there exists only one orbit passed by the polynomial over the ring and the orbit passes all the elements of the ring. Since a map which draws such only one orbit is called "one-stroke map" [4], we call such permutation polynomials "one-stroke polynomials" in this paper. The necessary and sufficient condition that specifies one-stroke polynomials with the assumption that the degree of the permutation polynomials are restricted to 1 or 2 is known [5]. One-stroke polynomials whose degrees are 1 or 2 are used in a linear congruential method and a quadratic congruential method, which are pseudo random number generators. A sufficient condition without any assumption has also been known [6], but a necessary and sufficient condition without the assumption has not been known as far as the authors know.

The other is more fundamental. In order to study about permutation polynomials over a ring of modulo 2^w, we should know which polynomials are permutation polynomials. The necessary and sufficient condition that specifies permutation polynomials have been already studied [7].

Based on the above, we study about the one-stroke polynomials over a ring of modulo 2^w whose degrees are *arbitrary.* This paper is constructed as follows. In Section 2, we introduce permutation polynomials over a ring of modulo 2^w. In Section 3, we derive the necessary and sufficient condition to specify one-stroke polynomials over the ring. In Section 4, we introduce some properties about one-stroke polynomials over the ring. Finally, we conclude this paper.

2. Permutation polynomials over a ring of modulo 2^w

In this section, we introduce permutation polynomials over a ring of modulo 2^w.

Definition 1 *A finite degree polynomial $f(X)$ with integer coefficients is called a permutation polynomial over a ring of modulo 2^w if*

$$\forall w \geq 0, \quad \{f(\bar{X}) \mod 2^w | \bar{X} \in \mathbb{Z}/2^w\mathbb{Z}\} = \mathbb{Z}/2^w\mathbb{Z}.$$

The necessary and sufficient condition that specifies permutation polynomials over the ring is given by the following theorem [7].

Theorem 2 (Rivest, 2001) *A polynomial $f(X) = \sum_{i=0}^{N} a_i X^i$, where the coefficients are integers, is a permutation polynomial over a ring of modulo 2^w if and only if*

$$a_1 \equiv 1 \mod 2, \tag{1}$$

$$(a_2 + a_4 + a_6 + \cdots) \equiv 0 \mod 2, \tag{2}$$

$$(a_3 + a_5 + a_7 + \cdots) \equiv 0 \mod 2. \tag{3}$$

The following lemma is used in order to prove Theorem 2. We use the lemma in the next section, again too.

Lemma 3 *Let $f(X)$ is a polynomial with integer coefficients. Then, $f(X)$ is a permutation polynomial over a ring of modulo 2^w if and only if*

$$\forall w \geq 1, \quad f(X + 2^{w-1}) \equiv f(X) + 2^{w-1} \mod 2^w.$$

The following lemma is also used in the next section.

Lemma 4 *Let $f(X)$ is a permutation polynomial over a ring of modulo 2^w. Then, $f^j(X)$ is also a permutation polynomial over the ring for arbitrary integer j, where $f^j(X) := f \circ f^{j-1}(X)$ and $f^1(X) := f(X)$.*

3. One-stroke polynomial

In this section, we derive a necessary and sufficient condition that coefficients of one-stroke polynomials over a ring of modulo 2^w satisfy. First, we exactly define one-stroke polynomials over a ring of modulo 2^w.

Definition 5 *Let $f(X)$ is a permutation polynomial over a ring of modulo 2^w. If $f(X)$ satisfy*

$$\forall w \geq 1, \quad \forall \bar{X}, \quad \{f^i(\bar{X}) \mod 2^w | i \in \mathbb{Z}/2^w\mathbb{Z}\} = \mathbb{Z}/2^w\mathbb{Z},$$

$f(X)$ is called a one-stroke polynomial over a ring of modulo 2^w.

Example 6 *We consider polynomials $F(X) = 4X^3 + X + 1$ and $G(X) = 6X^3 + 2X^2 + X + 1$. Both of them are permutation polynomials over a ring of modulo 2^w. Figs. 1 and 2 show orbits on a ring of modulo 2^w passed by $F(X)$ and $G(X)$, respectively. In Fig. 1, each orbit passes all the elements of the ring where the orbit is passed on. It means that $F(X)$ is a one-stroke polynomial over a ring of modulo 2^w. On the other hand, $G(X)$ is not a one-stroke polynomial over a ring of modulo 2^w because there is not an orbit which passes all elements of $\mathbb{Z}/2^3\mathbb{Z}$.*

Next, we introduce some lemmas. By the definition, the following two lemmas are obviously true.

Lemma 7 *Let $f(X)$ is a permutation polynomial over a ring of modulo 2^w. Then, $f(X)$ is a one-stroke polynomial over the ring if and only if*

$$f^i(0) \equiv 0 \mod 2^w \;\Leftrightarrow\; i \equiv 0 \mod 2^w.$$

Lemma 8 *Let $f(X)$ is a permutation polynomial over a ring of modulo 2^w. Then, $f(X)$ is a one-stroke polynomial over the ring if and only if*

$$f^{2^w}(0) \equiv 0 \mod 2^w,$$
$$f^{2^{w-1}}(0) \not\equiv 0 \mod 2^w.$$

Lemma 9 *Let $f(X)$ is a permutation polynomial over a ring of modulo 2^w. Then, $f(X)$ is a one-stroke polynomial over the ring if and only if*

$$\forall w \geq 1, \quad f^{2^{w-1}}(0) \equiv 2^{w-1} \mod 2^w. \tag{4}$$

Proof Assume that $f(X)$ is a one-stroke polynomial over the ring. By the definition,

$$\forall w \geq 1, \quad \exists i \leq 2^w, \text{ s.t. } f^i(0) \equiv 2^{w-1} \mod 2^w.$$

Then, by Lemma 3 and 4,

$$f^{2i}(0) \equiv f^i(2^{w-1}) \mod 2^w \equiv 0 \mod 2^w.$$

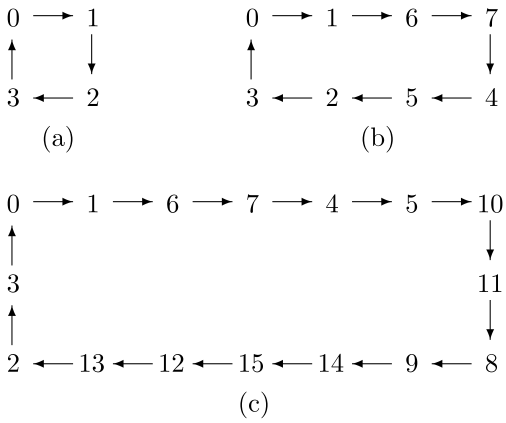

Fig. 1. Orbits passed by $F(X)$. (a) Orbit on $\mathbb{Z}/2^2\mathbb{Z}$. (b) Orbit on $\mathbb{Z}/2^3\mathbb{Z}$. (c) Orbit on $\mathbb{Z}/2^4\mathbb{Z}$.

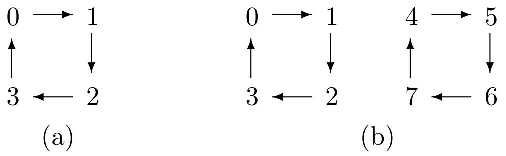

Fig. 2. Orbits passed by $G(X)$. (a) Orbit on $\mathbb{Z}/2^2\mathbb{Z}$. (b) Orbit on $\mathbb{Z}/2^3\mathbb{Z}$.

By Lemma 7, $2i = 2^w$. Then, $i = 2^{w-1}$.

Conversely, assume that (4) is true. Then, by Lemma 3 and 4,

$$f^{2^w}(0) \equiv f^{2^{w-1}}(2^{w-1}) \mod 2^w \equiv 0 \mod 2^w.$$

By Lemma 8, $f(X)$ is a one-stroke polynomial over the ring.

(QED)

Lemma 10 *Assume that $f(X)$ is a permutation polynomial over a ring of modulo 2^w and $f(X)$ satisfy $f^2(0) \equiv 2 \mod 4$ and $f^4(0) \equiv 4 \mod 8$. Then,*

$$\forall w \geq 2, \quad f^{2^{w-1}}(0) \equiv 2^{w-1} \mod 2^w.$$

Proof Assume that $f^2(X) = \sum b_i X^i$ and $f^4(X) = \sum c_i X^i$, where all b_i and c_i are integers. By the assumption of the lemma, $b_0 \equiv 2 \mod 4$ and $c_0 \equiv 4 \mod 8$. Since $f(X)$ is a permutation polynomial over the ring, by Lemma 4, $f^2(X)$ is also permutation polynomial over the ring. Then, by the Theorem 2, $b_1 \equiv 1 \mod 2$. Since $f^4(X) = f^2 \circ f^2(X)$,

$$\begin{aligned} c_1 &= b_1^2 + 2b_2b_1b_0 + 3b_3b_1b_0^2 + 4b_4b_1b_0^3 + \cdots \\ &\equiv b_1^2 \mod 4 \quad (\because b_0 \equiv 2 \mod 4) \\ &\equiv 1 \mod 4 \quad (\because b_1 \equiv 1 \mod 2). \end{aligned}$$

Assume that there exists an integer $\bar{w} \geq 3$ such that $f^{2^{\bar{w}-1}}(0) \equiv 2^{\bar{w}-1} \mod 2^{\bar{w}}$ and the first degree's coefficient of the $f^{2^{\bar{w}-1}}(X)$ is 1 under modulo 4. We express $f^{2^{\bar{w}-1}}(X)$ and $f^{2^{\bar{w}}}(X)$ as $f^{2^{\bar{w}-1}}(X) = \sum d_i X^i$ and $f^{2^{\bar{w}}}(X) = \sum e_i X^i$, where all d_i and e_i are integers. By the assumption, $d_1 \equiv 1 \mod 4$ and $d_0 \equiv 2^{\bar{w}-1} \mod 2^{\bar{w}}$.

$$e_1 = d_1^2 + 2d_2d_1d_0 + 3d_3d_1d_0^2 + 4d_4d_1d_0^3 + \cdots$$

$$\begin{aligned}
&\equiv d_1^2 \mod 4 \quad (\because d_0 \equiv 2^{\bar{w}-1} \mod 2^{\bar{w}})\\
&\equiv 1 \mod 4 \quad (\because d_1 \equiv 1 \mod 2),\\
e_0 &= d_0 + d_1 d_0 + d_2 d_0^2 + d_3 d_0^3 + \cdots\\
&\equiv d_0 + d_0 d_1 \mod 2^{\bar{w}+1} \quad (\because d_0 \equiv 2^{\bar{w}-1} \mod 2^{\bar{w}})\\
&\equiv 2^{\bar{w}} \mod 2^{\bar{w}+1} \quad (\because d_1 \equiv 1 \mod 4).
\end{aligned}$$

Then, $f^{2^{\bar{w}}}(0) \equiv 2^{\bar{w}} \mod 2^{\bar{w}+1}$ and the first degree's coefficient of $f^{2^{\bar{w}}}(X)$ is 1 under modulo 4.

From the above, the lemma is true. **(QED)**

Finally, we introduce a necessary and sufficient condition that specifies one-stroke polynomials over a ring of modulo 2^w.

Theorem 11 *Let $f(X) = \sum_{i=0}^{N} a_i X^i$ is a polynomial, where all a_i are integers. Then, $f(X)$ is a one-stroke polynomial over a ring of modulo 2^w if and only if*

$$\begin{aligned}
&a_0 \equiv 1 \mod 2,\\
&a_1 \equiv 1 \mod 2,\\
&(a_2 + a_4 + a_6 + \cdots) \equiv 0 \mod 2,\\
&(a_3 + a_5 + a_7 + \cdots) \equiv 2a_2 \mod 4,\\
&(a_1 + a_2 + a_3 + \cdots) \equiv 1 \mod 4.
\end{aligned}$$

Proof If $f(X)$ is a one-stroke polynomial over the ring, $f(X)$ is a permutation polynomial over the ring. Then, by Theorem 2, Lemmas 9 and 10, $f(X)$ is a one-stroke polynomial over the ring if and only if (1), (2), (3) and

$$\begin{aligned}
f(0) &\equiv 1 \mod 2,\\
f^2(0) &\equiv 2 \mod 4,\\
f^4(0) &\equiv 4 \mod 8.
\end{aligned}$$

Since $f(0) = a_0$,

$$f(0) \equiv 1 \mod 2 \Leftrightarrow a_0 \equiv 1 \mod 2.$$

Since $f^2(0) = a_0 + a_1 a_0 + a_2 a_0^2 + \cdots + a_N a_0^N$, if $a_0 \equiv 1 \mod 2$, (1) and (3),

$$\begin{aligned}
f^2(0) &\equiv a_0(1 + a_1 + a_3 + a_5 + \cdots)\\
&\quad + (a_2 + a_4 + a_6 + \cdots) \mod 4\\
&\equiv 1 + a_1 + a_2 + a_3 + \cdots + a_N \mod 4.
\end{aligned}$$

Then,

$$\begin{aligned}
&f^2(0) \equiv 2 \mod 4, \quad a_0 \equiv 1 \mod 2, \quad (1) \text{ and } (3)\\
&\Leftrightarrow (a_1 + a_2 + a_3 + \cdots) \equiv 1 \mod 4,\\
&\quad a_0 \equiv 1 \mod 2, \quad (1) \text{ and } (3).
\end{aligned}$$

We express $f^2(X)$ as $f^2(X) = \sum b_i X^i$, where all b_i are integers. If $f(X)$ is a permutation polynomial over the ring, $f^2(X)$ is also a permutation polynomial over the ring by Lemma 4, and so $b_1 \equiv 1 \mod 2$ by Theorem 2. If $b_0 \equiv 2 \mod 4$ and $b_1 \equiv 1 \mod 2$,

$$\begin{aligned}
f^4(0) &= b_0 + b_1 b_0 + b_2 b_0^2 + b_3 b_0^3 + \cdots\\
&\equiv 2(1 + b_1 + 2b_2) \mod 8.
\end{aligned}$$

If $a_0 \equiv 1 \mod 2$, (1), (2) and (3),

$$\begin{aligned}
b_2 &= a_2 a_1 + \sum_{i=2}^{N} a_i \left\{ \frac{i(i-1)}{2} a_1^2 a_0^{i-2} + i a_2 a_0^{i-1} \right\}\\
&\equiv a_2 + \sum_{i=2}^{N} a_i \left\{ \frac{i(i-1)}{2} + i a_2 \right\} \mod 2\\
&\equiv a_2 + \sum_{i=2}^{N} a_i \left\{ \frac{i(i-1)}{2} \right\} \mod 2 \quad (\because (3))\\
&\equiv a_2 + (a_3 + a_7 + a_{11} + \cdots)\\
&\quad + (a_2 + a_6 + a_{10} + \cdots) \mod 2\\
&\equiv (a_3 + a_7 + a_{11} + \cdots)\\
&\quad + (a_6 + a_{10} + a_{14} + \cdots) \mod 2,\\
b_1 &= a_1^2 + 2a_2 a_1 a_0 + 3a_3 a_1 a_0^2 + \cdots + N a_N a_1 a_0^N\\
&\equiv 1 + a_1(3a_3 + 5a_5 + 7a_7 + \cdots)\\
&\quad + a_1 a_0(2a_2 + 4a_4 + 6a_6 + \cdots) \mod 4\\
&\equiv 1 + a_1(3a_3 + a_5 + 3a_7 + \cdots)\\
&\quad + a_1 a_0(2a_2 + 2a_6 + 2a_{10} + \cdots) \mod 4\\
&\equiv 1 + 2a_1(a_3 + a_7 + a_{11} + \cdots)\\
&\quad + a_1(a_3 + a_5 + a_7 + \cdots)\\
&\quad + 2(a_2 + a_6 + a_{10} + \cdots) \mod 4\\
&\equiv 1 + 2a_2 + 2(a_3 + a_7 + a_{11} + \cdots)\\
&\quad + (a_3 + a_5 + a_7 + \cdots)\\
&\quad + 2(a_6 + a_{10} + a_{14} + \cdots) \mod 4.
\end{aligned}$$

Then,

$$f^4(0) \equiv 4 + 2\{2a_2 + (a_3 + a_5 + a_7 + \cdots)\} \mod 8.$$

Therefore,

$$\begin{aligned}
&f^4(0) \equiv 4 \mod 8, b_0 \equiv 2 \mod 4, \quad (1), (2) \text{ and } (3)\\
&\Leftrightarrow (a_3 + a_5 + a_7 + \cdots) \equiv 2a_2 \mod 4,\\
&\quad b_0 \equiv 2 \mod 4, \quad (1), (2) \text{ and } (3).
\end{aligned}$$

From the above, the theorem is true. **(QED)**

4. Some properties of one-stroke polynomials

In this section, we introduce some properties of one-stroke polynomials. We show computability of one-stroke polynomials. Under the assumption that the degree of one-stroke polynomial $f(X)$ is lower than w, we show that following values can be calculated with polynomial order times of w.

(A) $\bar{X}$ satisfying $\bar{Y} \equiv f(\bar{X}) \mod 2^w$ for given $\bar{Y}$.

(B) j satisfying $\bar{Y} \equiv f^j(\bar{X}) \mod 2^w$ for given $\bar{X}$ and $\bar{Y}$.

(C) $\bar{Y}$ satisfying $\bar{Y} \equiv f^j(\bar{X}) \mod 2^w$ for given $\bar{X}$ and j.

In the paper [8], similar problem for permutation polynomials over the ring is discussed. Here, we use not only properties of permutation polynomials over the ring but also those of one-stroke polynomials over the ring.

Method to calculate (A). The following algorithm can calculate (A).

(i) Set $X' \leftarrow 0$ and $m \leftarrow 1$.

(ii) If $\bar{Y} \not\equiv f(X') \mod 2^m$, $X' \leftarrow 2^{m-1}$.

(iii) If $m = w$, output X' and finish this algorithm. Else, $m \leftarrow m+1$ and return to (ii).

In the step (ii), if $\bar{Y} \equiv f(X') + 2^{m-1} \mod 2^m$, $\bar{Y} \equiv f(X' + 2^{m-1}) \mod 2^m$ by Lemma 3. Therefore, this algorithm can calculate (A).

Since the degree of $f(X)$ is lower than w, it requires $O(w)$ multiplications and $O(w)$ additions on $\mathbb{Z}/2^w\mathbb{Z}$ to calculate the value of $f(X) \mod 2^w$ for given X. Then, the calculation requires $O(w^3)$ times. Since the calculation is used $O(w)$ times in the above algorithm, the above algorithm requires $O(w^4)$ times.

Method to calculate (B). In order to calculate (B), we introduce polynomials $h_{2^i}(X)$ $(i = 0, 1, 2, \cdots, w-1)$ described as

$$h_{2^i}(X) := \left(f^{2^i}(X) \mod 2^w\right) \mod X^{\lceil \frac{w}{i} \rceil}.$$

The polynomials $h_{2^i}(X)$ have the following properties. If $\bar{X} \equiv 0 \mod 2^i$,

$$h_{2^i}(\bar{X}) \equiv f^{2^i}(\bar{X}) \mod 2^w.$$

If $\bar{X} \equiv 0 \mod 2^{i+1}$,

$$h_{2^i}(\bar{X}) \equiv 2^i \mod 2^{i+1},$$

and if $\bar{X} \equiv 2^i \mod 2^{i+1}$,

$$h_{2^i}(\bar{X}) \equiv 0 \mod 2^{i+1}.$$

If we know $h_{2^i}(X)$, we can calculate $h_{2^{i+1}}(X)$ as $h_{2^{i+1}}(X) = h_{2^i} \circ h_{2^i}(X) \mod X^{\lceil w/(i+1) \rceil}$. Because the degrees of $h_{2^i}(X)$ and $h_{2^{i+1}}(X)$ are lower than $\lceil w/i \rceil$, the calculation requires $O(\lceil w/i \rceil^3)$ multiplications and $O(\lceil w/i \rceil^3)$ additions. Then, the calculation requires $O(w^2 \lceil w/i \rceil^3)$ times. By the estimation, it takes $O(w^5)$ times to calculate the list $\{h_{2^0}(X), h_{2^1}(X), h_{2^2}(X), \ldots, h_{2^{w-1}}(X)\}$.

We show a method to calculate (B) by using $h_{2^i}(X)$. If we find j' and j'' such that

$$0 \equiv f^{j'}(\bar{Y}) \mod 2^w \text{ and } 0 \equiv f^{j''}(\bar{X}) \mod 2^w,$$

we can calculate as $j \equiv j'' - j' \mod 2^w$. We, therefore, assume that $\bar{Y}$ equals to 0 without loss of generality. Assume that $j = \sum_{i=0}^{w-1} \epsilon(i) 2^i$ where $\epsilon(i) \in \{0, 1\}$. Then, $f^j(\bar{X}) \equiv f^{\epsilon(w-1)2^{w-1}} \circ f^{\epsilon(w-2)2^{w-2}} \circ \cdots \circ f^{\epsilon(0)2^0}(\bar{X}) \mod 2^w$. By Lemma 7, if $f^j(X) \equiv 0 \mod 2^w$, $f^{\epsilon(m)2^m} \circ f^{\epsilon(m-1)2^{m-1}} \circ \cdots \circ f^{\epsilon(0)2^0}(\bar{X}) \equiv 0 \mod 2^{m+1}$ for arbitrary m. Then, by the properties of $h_{2^i}(X)$,

$$f^j(\bar{X}) \equiv h_{2^{w-1}}^{\epsilon(w-1)} \circ h_{2^{w-2}}^{\epsilon(w-2)} \circ \cdots \circ h_{2^0}^{\epsilon(0)}(\bar{X}) \mod 2^w.$$

From the above, the following algorithm outputs j satysfing $f^j(\bar{X}) \equiv 0 \mod 2^w$.

(1) Set $i \leftarrow 0$, $j \leftarrow 0$ and $X' = \bar{X}$.

(2) If $X' \equiv 2^i \mod 2^{i+1}$, $X' \leftarrow h_{2^i}(X') \mod 2^w$ and $j \leftarrow j + 2^i$.

(3) If $i = w-1$, output j and finish this algorithm. Else, $i \leftarrow i+1$ and return to step 2.

It takes $O(w^2 \lceil w/i \rceil)$ times to calculate the value of $h_{2^i}(\bar{X})$ for given $\bar{X}$. Then, this algorithm requires $O(w^3 \log w)$ times, but calculating (B) requires $O(w^5)$ because we must calculate the list $\{h_{2^0}(X), h_{2^1}(X), h_{2^2}(X), \ldots, h_{2^{w-1}}(X)\}$.

Method to calculate (C). By using the above algorithm, we can find j' such that $f^{j'}(\bar{X}) \equiv 0 \mod 2^w$, and so it is enough to show an algorithm to calculate $f^k(0) \mod 2^w$ for given k. Assume that $k = \sum_{i=0}^{w-1} \epsilon(i) 2^i$ where $\epsilon(i) \in \{0, 1\}$. Then, $f^k(0) \equiv f^{\epsilon(0)2^0} \circ f^{\epsilon(1)2^1} \circ \cdots \circ f^{\epsilon(w-1)2^{w-1}}(0) \mod 2^w$. By Lemma 7, $f^{\epsilon(m)2^m} \circ f^{\epsilon(m+1)2^{m+1}} \circ \cdots \circ f^{\epsilon(w-1)2^{w-1}}(0) \equiv 0 \mod 2^{m+1}$ for arbitrary m. Then, by the properties of $h_{2^i}(X)$,

$$f^k(0) \equiv h_{2^0}^{\epsilon(0)} \circ h_{2^1}^{\epsilon(1)} \circ \cdots \circ h_{2^{w-1}}^{\epsilon(w-1)}(0) \mod 2^w.$$

From the above, the following algorithm outputs $f^k(0) \mod 2^w$.

(1) Set $i \leftarrow w-1$, $X' = 0$.

(2) If $(i+1)$-th least significant bit of k is 1, $X' \leftarrow h_{2^i}(X') \mod 2^w$.

(3) If $i = 0$, output X' and finish this algorithm. Else, $i \leftarrow i-1$ and return to step 2.

This algorithm also requires $O(w^3 \log w)$ times, but calculating (C) requires $O(w^5)$ by the same reason why the method to calculate (B) requires $O(w^5)$ times.

5. Conclusion

We derived the necessary and sufficient condition to specify one-stroke polynomials over a ring of modulo 2^w. The condition enables us to construct many long sequences with maximum periods such that the distribution of points of the sequences are uniform over the ring. In addition, one-stroke polynomials have some interesting properties. One-stroke polynomials will be applied for many fields, including cryptography and pseudo random number generators.

References

[1] R. L. Rivest, M. J. B. Robshaw, R. Sidney and Y. L. Yin, The RC6 Block Cipher, https://people.csail.mit.edu/rivest/pubs/RRSY98.pdf.

[2] K. Umeno, S. Kim and A. Hasegawa, 128bit VSC Specification (in Japanese), http://www.chaosware.com/vsc128.pdf.

[3] A. Iwasaki and K. Umeno, Improving security of vector stream cipher, Nonlinear Theory Appl., **7** (2016), 30–37.

[4] K. Umeno, Complex systems and communication (in Japanese), in: Information systems as complex systems, Waseda University Advanced Institute for Complex Systems ed., pp. 181–250, Kyouritsu-syuppansya, Tokyo, 2007.

[5] D. E. Knuth, The Art of Computer Programming. Vol. 2, Addison-Wesley, Upper Saddle River, 1981.

[6] R. Coveyou, Random number generation is too important to be left to chance, Stud. Appl. Math., **3** (1970), 70–111.

[7] R. L. Rivest, Permutation polynomials modulo 2^w, Finite Fields Th. Appl., **7** (2001), 287–292.

[8] A. Iwasaki and K. Umeno, Three theorems on odd degree Chebyshev polynomials and more generalized permutation polynomials over a ring of module 2^w, arXiv:1602.08238v2, 2016.