JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **21**, No. 2, June 2008

ON A CHARACTERIZATION OF T-FUNCTIONS WITH ONE CYCLE PROPERTY

Min Surp Rhee*

Abstract. To the design of secret key, there are two types of basic approaches called the tame approach and the wild approach. In the tame approach we try to use only simple primitives such as linear feedback shift registers and to prove mathematical theorems about their cryptographic properties. In the wild approach we try to use crazy compositions of operations which mix a variety of domains in a nonlinear and nonalgebraic way. There are several papers which try to bridge this gap by considering semi-wild constructions. A T-function on n-bit words plays an important role in semi-wild constructions. In this paper we study the invertibility and the period of some T-functions. Especially we characterize some polynomials which has a single cycle property.

1. Introduction

There are two basic approaches to the design of secret key cryptographic schemes, which are known as the tame approach and the wild approach. In the tame approach we try to use only simple primitives such as linear feedback shift registers and to prove mathematical theorems about their cryptographic properties. In the wild approach we try to use crazy compositions of operations which mix a variety of domains in a nonlinear and nonalgebraic way. The first approach is typically preferred in textbooks and toy schemes, but the second approach is often used in real world designs. There are several papers which try to bridge this gap by considering semi-wild constructions. This construction looks

Received April 30, 2008; Accepted May 09, 2008.
2000 Mathematics Subject Classification: Primary 94A60.
Key words and phrases: T-function, n-bit words, period, a single cycle property, cryptographic scheme.
*The present research was conducted by the research fund of Dankook University in 2006.

like crazy combinations of boolean and arithmetic operations but analyzable mathematical properties. In these constructions we use T-functions which contain arbitrary compositions of plus, minus, times, or, and, xor operations on n-bit words. In this paper we study the invertibility and the period of some T-functions. Especially we will prove some propositions in an elementary way to characterize some polynomials which has a single cycle property.

2. Basic definitions and results

Let $\mathbb{B}^n = \{(x_{n-1}, x_{n-2}, \cdots, x_1, x_0) | x_i \in \mathbb{B}\}$ be the set of all n-tuples of elements in $\mathbb{B}$, where $\mathbb{B} = \{0, 1\}$. Then an element of $\mathbb{B}$ is called a bit and an element of $\mathbb{B}^n$ is called an n-bit word. An element x of $\mathbb{B}^n$ can be represented as $([x]_{n-1}, [x]_{n-2}, \cdots, [x]_0)$, where $[x]_{i-1}$ is the i-th component from the right end of x. It is often useful to express x as $\sum_{i=0}^{n-1} [x]_i 2^i$. In this expression every element x of $\mathbb{B}^n$ is considered as an element of $\mathbb{Z}_{2^n}$ and the set $\mathbb{B}^n$ as the set $\mathbb{Z}_{2^n}$, where $\mathbb{Z}_{2^n}$ is the congruence ring modulo 2^n. For example, an element $(0, 1, 1, 0, 1, 0, 0, 1)$ of $\mathbb{B}^8$ is considered as 105 in $\mathbb{Z}_{2^8} = \mathbb{Z}_{256}$.

Definition 2.1. For any n-bit words $x = (x_{n-1}, x_{n-2}, \cdots, x_1, x_0)$ and $y = (y_{n-1}, y_{n-2}, \cdots, y_1, y_0)$ of $\mathbb{B}^n$, we define the following:

(1) $x \pm y$ is defined as $x \pm y \mod 2^n$.

(2) xy is defined as $xy \mod 2^n$.

(3) $x \oplus y$ is defined as $z = (z_{n-1}, z_{n-2}, \cdots, z_1, z_0)$, where $z_i = 0$ if $x_i = y_i$ and $z_i = 1$ if $x_i \neq y_i$.

(4) $x \vee y$ is defined as $z = (z_{n-1}, z_{n-2}, \cdots, z_1, z_0)$, where $z_i = 0$ if $x_i = y_i = 0$ and $z_i = 1$ otherwise.

(5) $x \wedge y$ is defined as $z = (z_{n-1}, z_{n-2}, \cdots, z_1, z_0)$, where $z_i = 1$ if $x_i = y_i = 1$ and $z_i = 0$ otherwise.

Let $x = (0, 1, 1, 0, 1, 0, 0, 1)$ and $y = (0, 1, 0, 1, 1, 0, 0, 1)$ in $\mathbb{B}^8$. Then

$$x + y = (1, 1, 0, 0, 0, 0, 1, 0),\ x - y = (0, 0, 0, 1, 0, 0, 0, 0),$$

$$xy = (1, 0, 0, 0, 0, 0, 0, 1),\quad x \oplus y = (0, 0, 1, 1, 0, 0, 0, 0),$$

$$x \vee y = (0, 1, 1, 1, 1, 0, 0, 1),\ x \wedge y = (0, 1, 0, 0, 1, 0, 0, 1).$$

A function $f : \mathbb{B}^n \to \mathbb{B}^n$ is said to be a $\mathbf{T-function}$(short for a triangular function) if the k-th bit of an n-bit word $f(x)$ depends only on the first k bits of an n-bit word x.

EXAMPLE 2.2. *Let* $f(x) = x + (x^2 \vee 1)$. *If* $x = \sum_{i=0}^{n-1}[x]_i 2^i$, *then* $x^2 = [x]_0 + ([x]_1^2 + [x]_0[x]_1)2^2 + \cdots$ *and we have*

$$\begin{aligned}
&[f(x)]_0 = [x]_0 + [x]_0 \vee 1\\
&[f(x)]_1 = [x]_1\\
&[f(x)]_2 = [x]_2 + [x]_1 + [x]_0[x]_1\\
&\quad\vdots\\
&[f(x)]_i = [x]_i + \alpha_i,\ \ \alpha_i \text{ is a function of } [x]_0, \cdots, [x]_{i-1}\\
&\quad\vdots
\end{aligned}$$

Hence $f(x)$ *is a T-function. Also, for any given word* $f(x)$ *we can find* $[x]_0, [x]_1, \cdots, [x]_{n-1}$ *in order. Therefore* $f(x)$ *is an invertible T-function.*

A polynomial f over $\mathbb{Z}_{2^n}$ may be considered as a T-function. A polynomial over $\mathbb{Z}_{2^n}$ is a permutation polynomial if it is invertible on $\mathbb{Z}_{2^n}$. The following result is well known in [2].

PROPOSITION 2.3. *Let* $f(x) = a_0 + a_1x + \cdots + a_dx^d$ *be a polynomial over* $\mathbb{Z}_{2^n}$. *Then* $f(x)$ *is a permutation polynomial over* $\mathbb{Z}_{2^n}$ *if and only if* a_1 *is odd,* $a_2 + a_4 + \cdots$ *is even and* $a_3 + a_5 + \cdots$ *is even.*

Let $a_0, a_1, \cdots a_n, \cdots$ be a sequence of numbers(or words) in $\mathbb{Z}_{2^n}$. If there is the least positive integer r such that $a_{i+r} = a_i$ for each non-negative integer i, then $a_0, a_1, \cdots, a_{r-1}$ is called a cycle of period r. In general $a_i, a_{i+1}, \cdots, a_{i+r-1}$ is a cycle of period r for each i.

Now, for any function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$, let us define $f^i : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ by

$$f^i(x) = \begin{cases} x & \text{if } i = 0\\ f(f^{i-1}(x)) & \text{if } i \geq 1 \end{cases}$$

Note that if f is a bijective T-function then so does f^i for each i. A word α of $\mathbb{Z}_{2^n}$ has a cycle of period r in f if r is the least positive integer such that $f^r(\alpha) = \alpha$. If a word α has a cycle of period r in f, then α generates a cycle $\alpha = \alpha_0, \alpha_1, \cdots, \alpha_{r-1}$ of period r, where $\alpha_i = f^i(\alpha)$. Also, in this case every $\alpha_i (0 \leq i \leq r-1)$ has a cycle of period r. In particular a word which has a cycle of period 1 is called **a fixed word**. That is, a word α of $\mathbb{Z}_{2^n}$ in f is a fixed word if $f(\alpha) = \alpha$. Also, f is said to have **a single cycle property** if there is a word which has a cycle of period 2^n. In this case every word of $\mathbb{Z}_{2^n}$ has a cycle of period 2^n.

Consider a sequence of words

$$\alpha_0 = f^0(\alpha) = \alpha,\ \alpha_1 = f(\alpha), \cdots, \alpha_i = f^i(\alpha), \cdots, \alpha_m = f^m(\alpha), \cdots$$

where a word α of $\mathbb{Z}_{2^n}$ has a cycle of length r in f. Then the r words

$$\alpha_0 = f^0(\alpha) = \alpha,\ \alpha_1 = f(\alpha), \cdots, \alpha_i = f^i(\alpha), \cdots, \alpha_{r-1} = f^{r-1}(\alpha)$$

are repeated in the sequence $\alpha_0, \alpha_1, \cdots, \alpha_m, \cdots$. Since we may think a word as n bits, we may consider that a word α of $\mathbb{Z}_{2^n}$ which has a cycle of length r in f generates a binary sequence of period $n \cdot 2^r$. Hence a T-function f that has a single cycle property generates a binary sequence of period $n \cdot 2^n$, which is the longest period in f.

EXAMPLE 2.4. *Let $f(x) = 2x^2 + x$ in $\mathbb{Z}_{16}$. Then $f(0) = 0$ and $f(8) = 8$ imply that 0 and 8 are fixed words in f. Note $f(2) = 10$ and $f(10) = 2$. Hence 2 is a word which has a cycle of period 2. Note $f(1) = 3, f^2(3) = 5, \cdots, f^8(15) = 1$. Hence 1 is a word which has a cycle of period 8. Hence a word 1 in $\mathbb{Z}_{16}$ generates a binary sequence of period $8 \cdot 4$ in f. That is, '1 3 5 7 9 11 13 15' is a sequence of words, which may be represented as a binary sequence*

0001 0011 0101 0111 1001 1011 1101 1111

By a simple calculation we know that a function $f(x) = x + 1$ in $\mathbb{Z}_{16}$ has a single cycle property.

The following three propositions can be easily proved, whose proof may be found in [2].

PROPOSITION 2.5. *If a function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ has a single cycle property, then $\mathbb{Z}_{2^n} = \{f^i(x) | i \in \mathbb{Z}_{2^n}\}$ for each $x \in \mathbb{Z}_{2^n}$. In particular, $\mathbb{Z}_{2^n} = \{f^i(0) | i \in \mathbb{Z}_{2^n}\}$. Consequently, f is an invertible function on $\mathbb{Z}_{2^n}$.*

PROPOSITION 2.6. *Let f be an invertible T-function on $\mathbb{Z}_{2^n}$. Then for each cycle in f of period l on $\mathbb{Z}_{2^k}$, there are either two cycles of period l or one cycle of period $2l$ on $\mathbb{Z}_{2^{k+1}}$. Consequently, every cycle in f on $\mathbb{Z}_{2^n}$ is of period 2^i for some $i \leq n$.*

PROPOSITION 2.7. *A function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ has a single cycle property if and only if $f^{2^{n-1}}(0) = 2^{n-1} \bmod 2^n$ and $f^{2^n}(0) = 0 \bmod 2^n$.*

3. Length of cycles in some functions

In this section we find the period of cycles in some functions, which generate binary sequences with a cycle of period long enough. Also, we characterize some polynomials which have a single cycle property in an elementary way.

PROPOSITION 3.1. *Let $f(x) = x(2x+1) \bmod 2^n$. Then :*

(1) The number of fixed words in f is $2^{[\frac{n+1}{2}]}$, where $[x]$ is the greatest integer which is not greater than x.

(2) The number of words of period 2 in f is $2^{\frac{n}{2}}$ if n is even and 0 if n is odd.

Proof. (1) Let α be a fixed word of $f(x)$. Then we get

$$f(\alpha) = \alpha \bmod 2^n \text{ and } 2\alpha^2 = 0 \bmod 2^n$$

Hence $\alpha = 2^{\frac{n}{2}}k$ if n is even and $\alpha = 2^{\frac{n-1}{2}}k$ if n is odd for some nonnegative integer k. Thus the number of fixed words in f is $2^{\frac{n}{2}}$ if n is even and $2^{\frac{n+1}{2}}$ if n is odd.

Therefore the number of fixed words in f is $2^{[\frac{n+1}{2}]}$.

(2) Let α be a word of $f(x)$ of period ≤ 2. Then we get

$$f^2(\alpha) = \alpha \bmod 2^n \text{ and } 4\alpha^2(2\alpha^2 + 2\alpha + 1) = 0 \bmod 2^n$$

Hence $4\alpha^2 = 0 \bmod 2^n$ and so $\alpha^2 = 0 \bmod 2^{n-2}$. Thus similarly we can prove that the number of words of $f(x)$ of period ≤ 2 in f is $2^{\frac{n}{2}+1}$ if n is even and $2^{\frac{n+1}{2}}$ if n is odd. Therefore it follows from (1) that the number of words of period 2 in f is $2^{\frac{n}{2}}$ if n is even and 0 if n is odd. □

It is well known that the above function is used in RC6, which is one of 5 candidate algorithms that were chosen in the second test of AES(advanced encryption standard). But this function is very unsuitable for PRNG(pseudo random number generator). In this sense a function which has a single cycle property is important for PRNG.

PROPOSITION 3.2. *Let $f(x) = x + (x^2 \vee C) \bmod 2^n$ be a T-function. Then the following hold:*

(1) If f is invertible, then $[C]_0 = 1$.

(2) f has a single cycle property if and only if $[C]_0 = [C]_2 = 1$.

Proof. The proof may be found in [2]. □

Now, we characterize an affine function with a single cycle property.

PROPOSITION 3.3. *Suppose that both a and b are odd, and that $n \geq 2$. Then the following hold:*

(1) If $a = 1 \bmod 4$, then $f(x) = ax + b$ has a single cycle property.

(2) If $a = 3 \bmod 4$, then $f(x) = ax + b$ has no single cycle property.

Proof. Note that

$$f(0) = b,\ f^2(0) = b(a+1),\ \cdots,\ f^i(0) = (a^{i-1} + \cdots + a + 1)b,\ \cdots$$

(1) If $a = 1$, then $\{f^i(0)|i \in \mathbb{Z}_{2^n}\} = \{ib|i \in \mathbb{Z}_{2^n}\} = \mathbb{Z}_{2^n}$ since $(b, 2^n) = 1$. Hence the word 0 has a cycle of period 2^n. If $a \neq 1$, then $\{f^i(0)|i \in \mathbb{Z}_{2^n}\} = \{\frac{(a^i-1)b}{a-1}|i \in \mathbb{Z}_{2^n}\}$. If $n = 2$ and $a = 1 \bmod 4$, then $f(x)$ has a cycle of period 2^2. If $n = 3$, then $f(x) = 5x + b$. Note that $f^4(0) = \frac{(5^4-1)b}{4} = 4b = 4 \bmod 8$. Hence by Proposition 2.7 $f(x) = ax + b$ has a single cycle of period 8. Suppose that it holds for $n = k$. Then $f^{2^{k-1}}(0) = 0 \bmod 2^{k-1}$ and $f^{2^{k-1}}(0) \neq 0 \bmod 2^k$. So we have $\frac{(a^{2^{k-1}}-1)b}{a-1} = 0 \bmod 2^{k-1}$ and $\frac{(a^{2^{k-1}}-1)b}{a-1} \neq 0 \bmod 2^k$. Note that $a = 1 \bmod 4$ implies $(a^{2^{k-1}} + 1)b = 2 \bmod 4$. Hence we have

$$\frac{(a^{2^k} - 1)b}{a - 1} = \frac{(a^{2^{k-1}} - 1)}{a - 1} \cdot (a^{2^{k-1}} + 1)b \neq 0 \bmod 2^{k+1}.$$

Hence it holds for $n = k + 1$. Thus $f(x) = ax + b$ has a cycle of period 2^n. Therefore, $f(x) = ax + b$ has a single cycle property.

(2) If $n = 2$, then $f(x) = 3x + 1$ or $f(x) = 3x + 3$. In both cases we have $f^{2^1}(0) = 0 \bmod 2^2$. Hence $f(x) = ax + b$ has no cycle of period 2^2. Now assume that it holds for $n = k$. Then $f(x) = ax + b$ has no cycle of period 2^k. Hence $f(x)$ has a cycle of period at most 2^{k-1}. That is, $f^{2^{k-1}}(0) = 0 \bmod 2^k$. Hence we have

$$f^{2^{k-1}}(0) = \frac{(a^{2^{k-1}} - 1)b}{a - 1} = 0 \bmod 2^k \text{ and } (a^{2^{k-1}} - 1)b = 0 \bmod 2^k(a-1).$$

Note $(a^{2^k} - 1)b = (a^{2^{k-1}} + 1)(a^{2^{k-1}} - 1)b = 2t(a^{2^{k-1}} - 1)b = 0 \bmod 2^{k+1}(a - 1)$ for some t with $a^{2^{k-1}} + 1 = 2t$. Hence $f^{2^k}(0) = \frac{(a^{2^k}-1)b}{a-1} = 0 \bmod 2^{k+1}$ and so $f(x) = ax + b$ has no cycle of period 2^n for any odd numbers $a(\neq 1)$ and b in $\mathbb{Z}_{2^{k+1}}$.

Therefore, $f(x) = ax + b$ has no single cycle property. □

PROPOSITION 3.4. *$f(x) = ax + b$ has a single cycle property if and only if $a = 1$ mod 4 and $(b, 2) = 1$.*

Proof. Suppose that $a \neq 1 \bmod 4$ or $(b, 2) \neq 1$. Then we will show the following three cases : $a = 3 \bmod 4$, $a = 0 \bmod 2$ and $(b, 2) \neq 1$.

If $a = 3 \bmod 4$, then by Proposition 3.3 (2) $f(x)$ has no single cycle property. If $a = 0 \bmod 2$, then $f(x)$ is not invertible. So it has no single cycle property. If $(b, 2) \neq 1$, then b is even and so $f^l(0)$ is even for $l \in \mathbb{Z}_{2^n}$. Hence $\{f^i(0)|i \in \mathbb{Z}_{2^n}\} = \{ib|i \in \mathbb{Z}_{2^n}\} \neq \mathbb{Z}_{2^n}$. Thus $f(x)$ has no single cycle property. The converse of this theorem is shown in Proposition 3.3. □

Now, we will discuss a quadratic function with a single cycle property.

PROPOSITION 3.5. *Let $f(x) = ax^2+bx+c$ be a quadratic polynomial over $\mathbb{Z}_{2^n}$, where the coefficients of $f(x)$ are in $\mathbb{Z}_{2^2}$. Then $f(x)$ has a single cycle property if and only if $f(x)$ is either $2x^2+3x+1$ or $2x^2+3x+3$.*

Proof. Suppose that $f(x)$ has a single cycle property. Then f has no fixed word. Hence $f(0) \neq 0$ implies $c = 1$ or $c = 3$. Since f is invertible, for any distinct x and y we get $ax^2+bx+c \neq ay^2+by+c$. In fact we have $(x-y)\{a(x+y)+b\} \neq 0$ or $a(x+y)+b \neq 0$ for any distinct x and y. Hence a is even and b is odd. Thus there are four cases below:

$$f(x) = 2x^2+x+1,\ \ f(x) = 2x^2+x+3,$$

$$f(x) = 2x^2+3x+1,\ \ f(x) = 2x^2+3x+3.$$

In the first two cases we get $f^2(0) = 0 \bmod 2^2$. Hence by the 2nd proof of Proposition 3.3 the word 0 has a cycle of period 2 in $f(x) = 2x^2+x+1$ and $f(x) = 2x^2+x+3$. Hence $f(x)$ has no single cycle property. In the last two cases $f(x) = 2x^2+3x+1$ and $f(x) = 2x^2+3x+3$ the word 0 has a cycle of period 2^k for $k \leq 3$. Assume that in $f(x) = 2x^2+3x+1$ the word 0 has a cycle of period 2^k for $k \geq 3$. Then $f^{2^{k-1}}(0) = 0 \bmod 2^{k-1}$ and $f^{2^{k-1}}(0) \neq 0 \bmod 2^k$ (ie $f^{2^{k-1}}(0) = 2^{k-1} \bmod 2^k$). Consider

$$\begin{aligned}\{f^i(0)|i \in \mathbb{Z}_{2^k}\} &= \{0 = f^0(0), f^1(0), f^2(0), \cdots f^{2^{k-1}-1}(0), f^{2^{k-1}}(0) = 0 \\ &\quad + 2^{k-1}, \cdots, f^{2^k-1}(0) = 2^{k-1} + f^{2^{k-1}-1}(0)\} \\ &= \mathbb{Z}_{2^k}\end{aligned}$$

in $\mathbb{Z}_{2^k}$ and $f^{2^k}(0) = 0 \bmod 2^k$. Since $f^{2^{k-1}}(0) = 2^{k-1} \bmod 2^k$ we have $f^{2^{k-1}}(0) = 2^{k-1} + \alpha 2^k \bmod 2^{k+1}$ for some α.

Since $3 \cdot 2^{k-1} = 2^{k-1} + 2^k$ and $3\alpha \cdot 2^k = \alpha \cdot 2^k \bmod 2^{k+1}$ we get the following:

$$\begin{aligned}f^{2^{k-1}+1}(0) &= f(f^{2^{k-1}}(0)) \\ &= 2(2^{k-1} + \alpha 2^k)^2 + 3(2^{k-1} + \alpha 2^k) + 1 \bmod 2^{k+1} \\ &= 3 \cdot 2^{k-1} + 3 \cdot 2^k \alpha + 1 \bmod 2^{k+1} \\ &= f(0) + 2^{k-1} + (1+\alpha)2^k \bmod 2^{k+1}\end{aligned}$$

$$\begin{aligned}
f^{2^{k-1}+2}(0) &= f(f^{2^{k-1}+1}(0)) \\
&= \{2f(0)^2 + 3f(0) + 1\} + 2^{k-1} + \alpha 2^k \bmod 2^{k+1} \\
&= f^2(0) + 2^{k-1} + \alpha 2^k \bmod 2^{k+1} \\
f^{2^{k-1}+3}(0) &= f(f^{2^{k-1}+2}(0)) \\
&= \{2f^2(0)^2 + 3f^2(0) + 1\} + 2^{k-1} + (1+\alpha)2^k \bmod 2^{k+1} \\
&= f^3(0) + 2^{k-1} + (1+\alpha)2^k \bmod 2^{k+1} \\
&\vdots
\end{aligned}$$

and we can prove

$$f^{2^k}(0) = f(f^{2^{k-1}+2^{k-1}-1}(0)) = f^{2^{k-1}}(0) + 2^{k-1} + \alpha 2^k = 2^k \bmod 2^{k+1}$$

by induction. Hence the word 0 has a cycle of period 2^{k+1} in f. So $f(x) = 2x^2 + 3x + 1$ has a single cycle property. Similarly, we can prove $f(x) = 2x^2 + 3x + 3$ has a single cycle property. □

PROPOSITION 3.6. *Let $f(x) = ax^2 + bx + c$ be a polynomial over $\mathbb{Z}_{2^n}$, where the coefficients of $f(x)$ are in $\mathbb{Z}_{2^2}$. Then $f(x)$ has a single cycle property if and only if $f(x)$ is one of the four polynomials $x+1$, $x+3$, $2x^2+3x+1$ and $2x^2+3x+3$.*

Proof. If $a = 0 \bmod 4$, then by Proposition 3.4 $f(x)$ is either $x+1$ or $x+3$. If $a \neq 0 \bmod 4$, it follows from Proposition 3.5 that $f(x)$ is either $2x^2+3x+1$ or $2x^2+3x+3$. The converse is trivial by Proposition 3.4 and Proposition 3.5. □

Finally, we will study a polynomial with a single cycle property. The following proposition is proved in [3].

PROPOSITION 3.7. *A polynomial $f(x)$ has a single cycle modulo 2^n (for any $n \geq 3$) if and only if it has a single cycle modulo 8.*

Now, we will characterize quadratic functions with a single cycle property as shown in the following proposition.

PROPOSITION 3.8. *Let $f(x) = a_2x^2 + a_1x + a_0$ be a polynomial. Then $f(x)$ has a single cycle property if and only if $f(x) = g(x) + 4h(x)$, where $h(x)$ is an arbitrary polynomial of degree 2 and $g(x)$ is one of the four polynomials $2x^2+3x+1$, $2x^2+3x+3$, $4x^2+x+1$ and $4x^2+x+3$.*

Proof. It is easily proved that $2x^2+3x+1$, $2x^2+3x+3$, $4x^2+x+1$ and $4x^2+x+3$ have a single cycle property by Proposition 3.5 and Proposition 3.7. Now let $h(x) = b_2x^2 + b_1x + b_0$ be an arbitrary

polynomial of degree 2. Then $f(x) = (a_2+4b_2)x^2+(a_1+4b_1)x+a_0+4b_0$. In the first case of $g(x) = 2x^2+3x+1$, we get $f(x) = (2+4b_2)x^2+(3+4b_1)x+1+4b_0$ and so we get the following:

$$\begin{aligned}
f(0) &= 1 + 4b_0 \neq 0 \bmod 8 \\
f^2(0) &= (2+4b_2)(1+4b_0)^2 + (3+4b_1)(1+4b_0) + (1+4b_0) \\
&= 2 + 4b_2 + 3 + 4b_1 + 12b_0 + 1 + 4b_0 \\
&= 6 + 4(b_1+b_2) \bmod 8 \\
f^3(0) &= (2+4b_2)[6+4(b_1+b_2)]^2 + (3+4b_1)[6+4(b_1+b_2)] + (1+4b_0) \\
&= 2 + 4(b_1+b_2) + 1 + 4b_0 \\
&= 3 + 4(b_0+b_1+b_2) \bmod 8 \\
f^4(0) &= (2+4b_2)[3+4(b_0+b_1+b_2)]^2 + (3+4b_1)[3+4(b_0+b_1+b_2)] \\
&\quad + (1+4b_0) \\
&= 2 + 4b_2 + 1 + 4b_0 + 4b_2 + 1 + 4b_0 \\
&= 4 \bmod 8
\end{aligned}$$

Hence by Proposition 2.7 $f(x)$ has a single cycle property modulo 8 and so by Proposition 3.7 it has a single cycle property modulo 2^n. Similarly, we can prove that it hold for the remaining 3 cases. Therefore $f(x) = g(x) + 4h(x)$ has a single cycle property modulo 2^n for any $g(x)$ and $h(x)$.

Conversely, assume $f(x) = a_2x^2+a_1x+a_0$ has a single cycle property modulo 2^n. Then a_1 and a_0 are odd, and a_2 is even. Let us consider $f(x)$ on modulo 2^3. Then $a_0 = 1, 3, 5, 7 \bmod 8$, $a_1 = 1, 3, 5, 7 \bmod 8$ and $a_2 = 0, 2, 4, 6 \bmod 8$. From these cases we have

(1) $a_2 = 0 \bmod 4 : a_1 = 1 \bmod 4$ and $a_0 = 1 \bmod 2$

(2) $a_2 = 2 \bmod 4 : a_1 = 3 \bmod 4$ and $a_0 = 1 \bmod 2$

Therefore we have completely proved it. □

PROPOSITION 3.9. *Let $h(x)$ be an arbitrary polynomial and $g(x)$ be one of the four polynomials $2x^2+3x+1$, $2x^2+3x+3$, $x+1$ and $x+3$. Then $f(x) = g(x) + 4h(x)$ has a single cycle property.*

Proof. Note that all terms of $4h(x)$ affect 4 or 8 in $f^i(0)$. Hence, by a similar process shown in the proof of Proposition 3.7, $f(x)$ has a single cycle property. □

By taking an appropriate polynomial instead of $h(x)$ the results of Proposition 3.9 includes Proposition 3.3(1) and Proposition 3.8.

References

[1] Jin Hong, Dong Hoon Lee, Yongjin Yeom and Daewan Han, *A New Class of Single Cycle T-functions*, FSE 2005, LNCS 3557, 68-82, 2005.
[2] A Kilmov and A. Shamir, *A New Class of Invertible Mappings*, CHES 2002, LNCS 2523, 470-483, 2003.
[3] A Kilmov and A. Shamir, *Cryptographic Applications of T-Functions*, SAC 2003, LNCS 3006, 248-261, 2004.
[4] A Kilmov and A. Shamir, *New Cryptographic Primitives Based on Multiword T-Functions*, FSE 2004, LNCS 3017, 1-15, 2004.

*

Department of Mathematics
Dankook University
Cheonan 330-714, Republic of Korea
E-mail: msrhee@dankook.ac.kr