JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **28**, No. 2, May 2015
http://dx.doi.org/10.14403/jcms.2015.28.2.331

ON SINGLE CYCLE T-FUNCTIONS GENERATED BY SOME ELEMENTS

Min Surp Rhee*

Abstract. Invertible transformations over n-bit words are essential ingredients in many cryptographic constructions. When n is large such invertible transformations are usually represented as a composition of simpler operations such as linear functions, S-P networks, Feistel structures and T-functions. Among them we study T-functions which are probably invertible transformations and are very useful in stream ciphers. In this paper we study the number of single cycle T-functions satisfying some conditions and characterize single cycle T-functions on $(\mathbb{Z}_2)^n$ generated by some elements in $(\mathbb{Z}_2)^{n-1}$.

1. Introduction

There are many researches about T-functions since Klimov and Shamir have first proposed a T-function to construct MDS maps in block ciphers[6] in order to resist differential attacks. They are also used in stream ciphers to overcome LFSR's shortcoming.

Let $(\mathbb{Z}_2)^n = \{(x_0, x_1, \cdots, x_{n-1}) \,|\, x_i \in \mathbb{Z}_2\}$ be the set of all n-tuples of elements in $\mathbb{Z}_2 = \{0, 1\}$, where n is a positive integer. An element of $\mathbb{Z}_2$ is called *a bit* and an element of $(\mathbb{Z}_2)^n$ is called *an n-bit word*. Let $[x]_{i-1}$ be the i-th bit from the left end of n-bit word x. Then $x = ([x]_0, [x]_1, \cdots, [x]_{n-1})$. In particular, the first bit $[x]_0$ of x is called *the least bit of x*. It is often useful to express an element $([x]_0, [x]_1, \cdots, [x]_{n-1})$ of $(\mathbb{Z}_2)^n$ as an element $\sum_{i=0}^{n-1}[x]_i 2^i$ of $\mathbb{Z}_{2^n}$. In this expression every element of $(\mathbb{Z}_2)^n$ is considered as an element of $\mathbb{Z}_{2^n}$ and vice versa, where $\mathbb{Z}_{2^n}$ is the congruence ring modulo 2^n.

Received March 21, 2015; Accepted April 24, 2015.
2010 Mathematics Subject Classification: Primary 94A60.
Key words and phrases: a T-function, an n-bit word, period, a boolean function, a single cycle T-function.
The present research was conducted by the research fund of Dankook University in 2014.

Consequently $(\mathbb{Z}_2)^n$ is considered as $\mathbb{Z}_{2^n}$ and vice versa. So an element of $\mathbb{Z}_{2^n}$ can be considered as an n-bit word. For example, an 8-bit word $(1,1,0,1,0,0,1,0)$ of $(\mathbb{Z}_2)^8$ is considered as an element 75 of $\mathbb{Z}_{2^8} = \mathbb{Z}_{256}$ and an element 135 of $\mathbb{Z}_{2^8}$ is considered as an 8-bit word $(1,1,1,0,0,0,0,1)$ of $(\mathbb{Z}_2)^8$.

Definition 1.1. For any n-bit words $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$ of $\mathbb{Z}_{2^n}$ we define the following binary operations:

(1) $x \pm y$ and xy are defined as $x \pm y \bmod 2^n$ and $xy \bmod 2^n$, respectively.

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

A function $f : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^n$ is called *a function f on* $(\mathbb{Z}_2)^n$. A function f on $(\mathbb{Z}_2)^n$ is said to be *a T-function*(short for a triangular function) if for each $k \in \{1, 2, \cdots, n\}$ the k-th bit $[f(x)]_{k-1}$ of an n-bit word $f(x)$ depends only on the first k bits $[x]_0, [x]_1, \cdots, [x]_{k-1}$ of an n-bit word x.

A sequence $a_0, a_1, \cdots, a_m, \cdots$ of n-bit words in $\mathbb{Z}_{2^n}$ is said to be of *period l* if there is the least positive integer l such that $a_{i+l} = a_i$ for every nonnegative integer i . Now, for a given function f on $\mathbb{Z}_{2^n}$ and a nonnegative integer i, we define a function $f^i : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ by

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

If f is a T-function on $\mathbb{Z}_{2^n}$, then so is f^i for every nonnegative integer i. Hence, if f is a bijective T-function on $\mathbb{Z}_{2^n}$, then so is f^i for every nonnegative integer i. An n-bit word a of $\mathbb{Z}_{2^n}$ is said to *have a cycle of period l* in a T-function f on $\mathbb{Z}_{2^n}$ if l is the least positive integer such that $f^l(a) = a$. If a has a cycle of period l in f, then a is said to *generate a sequence $a = a_0, a_1, \cdots, a_{l-1}, \cdots$ of period l*, where $a_i = f^i(a)$ for each nonnegative integer i. It is easy to show that every word $a_i (0 \leq i \leq l-1)$ has a cycle of period l if a_0 has a cycle of period l. In particular, a word which has a cycle of period 1 is called *a fixed word.*
For example, let $f(x) = 3x + 2$ on $\mathbb{Z}_{2^3}$. Then 3, 7 are fixed words, 2 generates a sequence 2, 0, 2, 0, $\cdots$ and 1 generates a sequence 1, 5, 1, 5, $\cdots$.

A T-function f on $\mathbb{Z}_{2^n}$ is said to have *a single cycle property* if there is an n-bit word which has a cycle of period 2^n. A T-function f on $\mathbb{Z}_{2^n}$ with a single cycle property is called *a single cycle T-function* on $\mathbb{Z}_{2^n}$. From this definition if f is a single cycle T-function on $\mathbb{Z}_{2^n}$, then every word of $\mathbb{Z}_{2^n}$ has a cycle of period 2^n and f is a bijective T-function on $\mathbb{Z}_{2^n}$.

EXAMPLE 1.2. Let f be a function on $\mathbb{Z}_{2^3}$ defined by $f(x) = 5x + 3$. Then $f(0) = 3, f(3) = 2, f(2) = 5, f(5) = 4, f(4) = 7, f(7) = 6, f(6) = 1$ and $f(1) = 0$. Hence 0 generates a sequence 0, 3, 2, 5, 4, 7, 6, 1, 0, $\cdots$ of period 8. Hence f is a single cycle T-function on $\mathbb{Z}_{2^3}$. If we represent an element of $\mathbb{Z}_{2^3}$ as an element of $(\mathbb{Z}_2)^3$ in an above sequence, then (0,0,0) generates a sequence (0,0,0), (0,1,1), (0,1,0), (1,0,1), (1,0,0), (1,1,1), (1,1,0), (1,0,0), (0,0,0), $\cdots$ of period 8, which may be considered as a binary sequence of period 3×2^3:

$$000011010101100111110001000\cdots$$

2. The number of T-functions

As we know, a boolean function on $(\mathbb{Z}_2)^n$ is a function from $(\mathbb{Z}_2)^n$ to $\mathbb{Z}_2$. We can also represent a function on $(\mathbb{Z}_2)^n$ as n boolean functions on $(\mathbb{Z}_2)^n$. Let f be a function on $(\mathbb{Z}_2)^n$ defined by $f(x) = y$, where $x, y \in (\mathbb{Z}_2)^n$. If $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$, then $y_i = [y]_i = [f(x)]_i = [f(x_0, x_1, \cdots, x_{n-1})]_i$ for all integers $i = 0, 1, \cdots, (n-1)$. We usually denote by $x_i = [x]_i$, $y_i = [y]_i = [f(x)]_i = f_i(x)$ and $f = (f_0, f_1, \cdots, f_{n-1})$, where f_i is a boolean function on $(\mathbb{Z}_2)^{i+1}$. If f is a T-function on $(\mathbb{Z}_2)^n$, then $[f(x)]_i = f_i([x]_0, [x]_1, \cdots, [x]_i)$ for every nonnegative integer i.

Let $\alpha_0(x) = 1$ be the constant function, and let α_i define a boolean function on $(\mathbb{Z}_2)^i$ for each positive integer i. For any real number a. we define an integer $[a]$ by the greatest integer which is not greater than a.

The following two results are well known in [4].

PROPOSITION 2.1. *A function f on $(\mathbb{Z}_2)^n$ is a single cycle T-function if and only if for every nonegative integer $i < n$ the $(i + 1)$-th bit of the output $f(x)$ can be represented as*

$$[f(x)]_i = [x]_i \oplus \alpha_i([x]_0, [x]_1, \cdots, [x]_{i-1})$$

for some boolean function α_i on $(\mathbb{Z}_2)^i$ satisfying $\alpha_0(x) = 1$ and $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = 1$.

PROPOSITION 2.2. *A polynomial $f(x)$ is a single cycle T-function on $(\mathbb{Z}_2)^n$ for any positive integer n if and only if it is a single cycle T-function on $(\mathbb{Z}_2)^3$.*

Proposition 2.3. *The number of all single cycle T-functions on* $(\mathbb{Z}_2)^n$ *is* 2^{2^n-n-1} .

Proof. By Proposition 2.1 for each single cycle T-function f on $(\mathbb{Z}_2)^n$ there are boolean functions $\alpha_0, \cdots, \alpha_{n-1}$ such that $\alpha_0(x) = 1$ and $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = 1$ for all $i = 1, 2, \cdots, n-1$. Note that $\alpha_0(x) = 1$ and $\alpha_i(x)$ is an algebraic normal form of $[x]_0, [x]_1, \cdots, [x]_{i-1}$, which is $\alpha_i(x) = c \oplus c_0[x]_0 \oplus c_1[x]_1 \oplus \cdots \oplus c_{i-1}[x]_{i-1} \oplus c_{0,1}[x]_0[x]_1 \oplus \cdots \oplus c_{0,1,\cdots,(i-1)}[x]_0[x]_1 \cdots [x]_{i-1}$ for each $i \geq 1$. So there are 2^i coefficients in $\alpha_i(x)$. Since $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = c_{0,1,\cdots,(i-1)} = 1$, all coefficients except $c_{0,1,\cdots,(i-1)}$ are arbitrary. Hence the number of all boolean functions α_i on $(\mathbb{Z}_2)^i$ satisfying $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = 1$ is 2^{2^i-1}. Let T_n be the number of all single cycle T-functions on $(\mathbb{Z}_2)^n$. Note that T_n depends on the number of the functions α_i for all $i = 0, 1, \cdots, n-1$. Since $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ is independent for each i we get

$$\begin{aligned} T_n &= \prod_{i=1}^{n-1} \text{the number of } \alpha_i \\ &= \prod_{i=1}^{n-1} 2^{2^i-1} = 2^{2^1+2^2+\cdots+2^{n-1}-(n-1)} = 2^{2^n-n-1}. \end{aligned}$$

□

Proposition 2.4. *Let* f *be a function on* $\mathbb{Z}_{2^n}$ *defined by* $f(x) = ax + b$. *Then* f *is a single cycle T-function if and only if* $a \equiv 1 \bmod 4$ *and* $b \equiv 1 \bmod 2$. *Consequently, the number of single cycle affine T-functions on* $\mathbb{Z}_{2^n}$ *is* 2^{2n-3}, *where* $n \geq 2$.

Proof. By Proposition 2.2 $f(x) = ax + b$ is a single cycle T-function on $\mathbb{Z}_{2^n}$ if and only if it is a single cycle T-function on $\mathbb{Z}_{2^3}$. If f is a single cycle T-function on $\mathbb{Z}_{2^3}$, then by Proposition 2.1 $[f(x)]_i = [x]_i \oplus \alpha_i(x)$ with $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = 1$ for all $i = 0, 1, 2$. If $i = 0$, then $[f(x)]_0 = [ax + b]_0 = [a]_0[x]_0 \oplus [b]_0$. Hence both a and b are odd. If $i = 1$, then $\alpha_1(x) = [a]_1[x]_0 \oplus [b]_1 \oplus [\frac{f_0(x)}{2}]$, where $f_0(x_0) = [x]_0 \oplus 1$. Note that $\bigoplus_{x=0}^{2^1-1} \alpha_1(x) = [a]_1 \oplus 1$. Hence $[a]_1 = 0$ and $[b]_1$ is arbitrary. If $i = 2$, then $\alpha_2(x) = [a]_2[x]_0 \oplus [b]_2 \oplus [\frac{f_1(x)}{2}]$, where $f_1(x) = [x]_1 \oplus [b]_1 \oplus [\frac{f_0(x)}{2}]$. Note that $\bigoplus_{x=0}^{2^2-1} \alpha_2(x) = 1$. Hence $[a]_2, [b]_1$, and $[b]_2$ are arbitrary. Hence $a \equiv 1 \bmod 4$ and $b \equiv 1 \bmod 2$. Conversely, if $a \equiv 1 \bmod 4$ and $b \equiv 1 \bmod 2$, then it is clear that f is a single cycle T-function on $\mathbb{Z}_{2^3}$. Hence f is a single cycle T-function on $\mathbb{Z}_{2^n}$. Now, assume $ax+b \equiv a'x+b'$

mod 2^n for every element x in $\mathbb{Z}_{2^n}$. By substituting $x = 0$ we get $b = b'$ in $\mathbb{Z}_{2^n}$. Hence $a = a'$ in $\mathbb{Z}_{2^n}$. Therefore, the number of single cycle affine T-functions on $\mathbb{Z}_{2^n}$ is $2^{n-2}2^{n-1} = 2^{2n-3}$, where $n \geq 2$. $\square$

PROPOSITION 2.5. *Let f be a function on $\mathbb{Z}_{2^n}$ defined by $f(x) = ax^2 + bx + c$. Then f is a single cycle T-function if and only if a, b and c in $\mathbb{Z}_{2^n}$ satisfy one of the following:*

(i) *$a \equiv 0$ mod 4, $b \equiv 1$ mod 4 and $c \equiv 1$ mod 2.*
(ii) *$a \equiv 2$ mod 4, $b \equiv 3$ mod 4 and $c \equiv 1$ mod 2.*

Proof. By Proposition 2.2 f is a single cycle T-function on $\mathbb{Z}_{2^n}$ if and only if it is a single cycle T-function on $\mathbb{Z}_{2^3}$. If f is a single cycle T-function on $\mathbb{Z}_{2^3}$, then by Proposition 2.1 $[f(x)]_i = f_i([x]_0, \cdots, [x]_i) = [x]_i \oplus \alpha_i(x)$ with $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = 1$ for all $i = 0, 1, 2$. If i=0, then $[f(x)]_0 = [ax^2 + bx + c]_0 = ([a]_0 \oplus [b]_0)[x]_0 \oplus [c]_0$. Hence both $a + b$ and c are odd. If $i = 1$, then $[f(x)]_1 = [ax^2 + bx + c]_1 = [b]_0[x]_1 \oplus \alpha_1(x)$. So $[b]_0 = 1$ and so $[a]_0 = 0$. Note that $\alpha_1(x) = ([a]_1 \oplus [b]_1)[x]_0 \oplus [c]_1 \oplus [\frac{f_0(x)}{2}]$ where $f_0(x) = [x]_0 \oplus 1$. Since $\bigoplus_{x=0}^{2^1-1} \alpha_1(x) = [a]_1 \oplus [b]_1 \oplus 1 = 1$. Hence $[a]_1 \oplus [b]_1$ is even and $[c]_1$ is arbitrary. If $i = 2$, then $[f(x)]_2 = [ax^2 + bx + c]_2 = [x]_2 \oplus \alpha_2(x)$, where $\alpha_2(x) = ([a]_2 \oplus [b]_2)[x]_0 \oplus [b]_1[x]_1 \oplus [c]_2 \oplus [\frac{[f(x)]_1}{2}]$. Note that $\bigoplus_{x=0}^{2^2-1} \alpha_2(x) = 1$ for any arbitrary $[a]_1$, $[a]_2$, $[b]_1$, $[b]_2$, $[c]_2$ and $[c]_2$. Hence we have the following two cases:

(i) $a \equiv 0$ mod 4, $b \equiv 1$ mod 4 and $c \equiv 1$ mod 2.
(ii) $a \equiv 2$ mod 4, $b \equiv 3$ mod 4 and $c \equiv 1$ mod 2.

Conversely, suppose that above two cases hold. Then it is clear that f is a single cycle T-function on $\mathbb{Z}_{2^3}$. Hence f is a single cycle T-function on $\mathbb{Z}_{2^n}$. $\square$

PROPOSITION 2.6. *Let $f(x) = ax^2 + bx + c$ be a T-function on $\mathbb{Z}_{2^n}$, where $n \geq 3$. Then $f(x)$ is a single cycle T-function if and only if there are elements $a \in \mathbb{Z}_{2^{n-1}}$ and $b, c \in \mathbb{Z}_{2^n}$ which satisfy one of the following:*

(i) *$a \equiv 0$ mod 4, $b \equiv 1$ mod 4 and $c \equiv 1$ mod 2.*
(ii) *$a \equiv 2$ mod 4, $b \equiv 3$ mod 4 and $c \equiv 1$ mod 2.*

Proof. Suppose that (i) and (ii) are satisfied. Then by Proposition 2.5 $f(x)$ is a single cycle T-function. Conversely, let $f(x) = ax^2 + bx + c$ be a single cycle T-function on $\mathbb{Z}_{2^n}$. Then by Proposition 2.5 a, b and c in $\mathbb{Z}_{2^n}$ satisfy one of the following:

(i) $a \equiv 0$ mod 4, $b \equiv 1$ mod 4 and $c \equiv 1$ mod 2.
(ii) $a \equiv 2$ mod 4, $b \equiv 3$ mod 4 and $c \equiv 1$ mod 2.

Since $2^{n-1}x(x-1) \equiv 0 \bmod 2^n$ for every element x in $\mathbb{Z}_{2^n}$ we get

$$(a+2^{n-1})x^2 + bx + c \equiv ax^2 + (b+2^{n-1})x + c \bmod 2^n$$

for every element a in $\mathbb{Z}_{2^n}$. Hence every single cycle T-function with $a \geq 2^{n-1}$ can be replaced by $a - 2^{n-1}$. Hence every element can be assumed less than 2^{n-1}. So two conditions in Proposition 2.5 can be replaced by two conditions in Proposition 2.6. □

In the process of the proof of Proposition 2.6 every single cycle T-function of the form $bx + c \bmod 2^n$ can be replaced by a single cycle T-function of the form $2^{n-1}x^2 + (b+2^{n-1})x + c \bmod 2^n$. Hence every single cycle T-function of degree 1 can be replaced by a single cycle T-function of degree 2.

Proposition 2.7. *Suppose that $ax^2 + bx + c \equiv a'x^2 + b'x + c'$ mod 2^n for every element $x \in \mathbb{Z}_{2^n}$, where $a, a' \in \mathbb{Z}_{2^{n-1}}$ and $b, c, b', c' \in \mathbb{Z}_{2^n}$ satisfy one of the following:*

(i) *$a \equiv 0$ mod 4, $b \equiv 1$ mod 4 and $c \equiv 1$ mod 2.*
(ii) *$a \equiv 2$ mod 4, $b \equiv 3$ mod 4 and $c \equiv 1$ mod 2.*

Then $a \equiv a'$ mod 2^{n-1}, $b \equiv b'$ mod 2^n and $c \equiv c'$ mod 2^n. Consequently, the number of single cycle T-functions on $\mathbb{Z}_{2^n}$ of degree $n \leq 2$ is 2^{3n-5}, where $n \geq 3$.

Proof. Suppose that $(a-a')x^2 + (b-b')x + (c-c') \equiv 0 \bmod 2^n$ for every element $x \in \mathbb{Z}_{2^n}$. By substituting $x = 0$, we get $c \equiv c' \bmod 2^n$. Hence $(a-a')x^2 + (b-b')x \equiv 0 \bmod 2^n$ for every element $x \in \mathbb{Z}_{2^n}$. Without loss of generality we may assume $a \geq a'$. So $0 \leq a - a' < 2^{n-1}$. By substituting $x = 1$ and $x = -1$, we get

$$(a-a') + (b-b') \equiv 0 \bmod 2^n \text{ and } (a-a') - (b-b') \equiv 0 \bmod 2^n.$$

Hence $2(a-a') \equiv 0 \bmod 2^n$ and so $a - a' \equiv 0 \bmod 2^{n-1}$. Consequently, $b \equiv b' \bmod 2^n$. Therefore, the number of single cycle T-functions of degree ≤ 2 is $2 \cdot 2^{n-3}2^{n-2}2^{n-1} = 2^{3n-5}$. □

Example 2.8. By Proposition 2.3 and Proposition 2.4 every single cycle T-function on $\mathbb{Z}_{2^2}$ is a single cycle T-function of degree 1. Similarly by Proposition 2.3 and Proposition 2.7 every single cycle T-function on $\mathbb{Z}_{2^3}$ may be expressed as a single cycle T-function of degree 2.

3. Single cycle T-functions generated by some elements

In Proposition 2.1 we explain that a function f on $(\mathbb{Z}_2)^n$ is a single cycle T-function if and only if for every nonegative integer $i < n$ the $(i+1)$-th bit of the output $f(x)$ can be represented as

$$[f(x)]_i = [x]_i \oplus \alpha_i \text{ for some boolean function } \alpha_i \text{ on } (\mathbb{Z}_2)^i$$

satisfying $\alpha_0(x) = 1$ and $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = 1$. In this case we say that a function f is *a single cycle T-function on $\mathbb{Z}_{2^n}$ determined by* $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$, where
$\alpha_0(x) = 1$ and α_i is a boolean function on $(\mathbb{Z}_2)^i$
with $\bigoplus_{x=0}^{2^i-1} \alpha_i(x) = 1$ for every positive integer $i \le n-1 \cdots\cdots (*)$.

In this section we characterize single cycle T-functions determined by some special types of $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ satisfying $(*)$.

Let $x = a_{n-2}a_{n-3}\cdots a_1 a_0$ be an element of $\mathbb{Z}_{2^{n-1}}$, and consider n boolean functions $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ which are defined as follows:

$$\alpha_0(x) = 1, \text{and}$$

$$\alpha_i(x) = \begin{cases} 1 & \text{if } x = a_{i-1}a_{i-2}\cdots a_0 \\ 0 & \text{if otherwise} \end{cases} \quad \text{for all } i = 1, 2, \cdots, n-1. \cdots\cdots (**)$$

Then $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ satisfy $(*)$. We say that $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ satisfying $(**)$ are *functions determined by* $a_{n-2}a_{n-3}\cdots a_1 a_0$. For example, n functions $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ determined by $0\cdots0101$ are boolean functions as follows:

$$\alpha_0(x) = 1, \ \alpha_1(x) = \alpha_2(x) = \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{otherwise} \end{cases} \quad \text{and}$$

$$\alpha_i(x) = \begin{cases} 1 & \text{if } x = 5 \\ 0 & \text{otherwise} \end{cases} \quad \text{for all } i \ge 3.$$

A single cycle T-function determined by functions $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ satisfying $(**)$ is shortly called *a single cycle T-function determined by* $a_{n-2}a_{n-3}\cdots a_1 a_0$.

Example 3.1. Let's consider a single cycle T-function generated by $0 = 00\cdots0$. Then $\alpha_0(x) = 1$ and $\alpha_i(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{otherwise} \end{cases}$ for all $i \ge 1$. If x is odd, then $\alpha_i(x) = 0$ for all $i \ge 1$. Hence $[f(x)]_0 = [x]_0 \oplus \alpha_0(x) = [x]_0 \oplus 1 = 0$ and $[f(x)]_i = [x]_i \oplus \alpha_i(x) = [x]_i$ for all $i \ge 1$. Hence $f(x) \equiv x - 1 \bmod 2^n$. Clearly $f(0) \equiv 2^n - 1 \equiv x - 1 \bmod 2^n$. If x is nonzero even, then $x = x_{n-1} \cdots x_{k+1} 10 \cdots 0$ and

$$[f(x)]_i = [x]_i \oplus \alpha_i(x) = [x]_i \oplus \begin{cases} 1 & \text{if } i \leq k \\ 0 & \text{if } i > k. \end{cases}$$

Hence $f(x) = x_{n-1} \cdots x_{k+1} 01 \cdots 1$ and $f(x) \equiv x - 1 \bmod 2^n$. Therefore, $f(x) \equiv x - 1 \bmod 2^n$.

EXAMPLE 3.2. Let's consider a single cycle T-function generated by $2^{n-1} - 1 = 11 \cdots 1$. Then $\alpha_0(x) = 1$ and $\alpha_i(x) = \begin{cases} 1 & \text{if } x = 2^i - 1 \\ 0 & \text{otherwise} \end{cases}$ for all $i \geq 1$. If x is even, then $\alpha_0(x) = 1$ and $\alpha_i(x) = 0$ for all $i \geq 1$. Hence $f(x) \equiv x + 1 \bmod 2^n$. Clearly, $f(2^n - 1) = 0$. If x is odd, then $x = x_{n-1} \cdots x_{k+1} 01 \cdots 1$ and

$$[f(x)]_i = [x]_i \oplus \alpha_i(x) = [x]_i \oplus \begin{cases} 1 & \text{if } i \leq k \\ 0 & \text{if } i > k. \end{cases}$$

Hence $f(x) = x_{n-1} \cdots x_{k+1} 10 \cdots 0$ and $f(x) \equiv x + 1 \bmod 2^n$. Therefore, $f(x) \equiv x + 1 \bmod 2^n$.

Now, we characterize the single cycle T-function on $\mathbb{Z}_{2^n}$ determined by an element $a_{n-2} a_{n-3} \cdots a_1 a_0$ in $\mathbb{Z}_{2^{n-1}}$.

THEOREM 3.3. *Let f be a single cycle T-function generated by $a = 2^{n-1} - 2^i$, where $1 \leq i \leq n - 1$. Then*

$$f(x) \equiv \begin{cases} x - 2a - 1 \bmod 2^n & \text{if } x \equiv 0 \bmod 2^i \\ x - 1 \bmod 2^n & \text{otherwise} \end{cases}.$$

Proof. If $a = 2^{n-1} - 2^i$, then $a_{n-2} = \cdots = a_i = 1$ and $a_{i-1} = \cdots = a_0 = 0$. Note that a single cycle T-function generated by a has n functions α_i as follows: $\alpha_0(x) = 1$, $\alpha_k(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{otherwise} \end{cases}$ for all k with $1 \leq k \leq i$ and $\alpha_k(x) = \begin{cases} 1 & \text{if } x = 2^k - 2^i \\ 0 & \text{otherwise} \end{cases}$ for all $k > i$. Let $x = x_{n-1} \cdots x_1 x_0$ and l be the least nonnegative integer such that $x_l \neq a_l$. If $l < i$, then $x_l = 1$ and $x_t = 0$ for all $t < l$. Hence

$$y_t = \begin{cases} x_t \oplus 1 & \text{if } t \leq l \\ x_t & \text{if } t > l \end{cases}$$

and $f(x) \equiv x-1 \bmod 2^n$. If $l \geq i$, then $x_l = 0$ and $x_t = a_t$ for all $t < l$. Hence $y_t = \begin{cases} x_t \oplus 1 & \text{if } t \leq l \\ x_t & \text{if } t > l \end{cases}$ and $f(x) \equiv x + 2^i + \cdots 2 + 1 \equiv x + 2^{i+1} - 1 \bmod 2^n$. If there is no l such that $x_l \neq a_l$, then $y_t = x_t \oplus 1$ for all t. Hence $f(x) \equiv x + 2^i + \cdots 2 + 1 \equiv x + 2^{i+1} - 1 \bmod 2^n$. Note that $x \equiv 0 \bmod 2^i$ if and only if $l \geq i$ or there is no l such that $x_l \neq a_l$. Since $2^{i+1} \equiv -2a \bmod 2^n$, Theorem 3.3 holds. □

Example 3.4. Let $n = 5$ and $i = 3$. Then

$$f(x) = \begin{cases} x + 2^4 - 1 \bmod 2^5 & \text{if } x \equiv 0 \bmod 2^3 \\ x - 1 \bmod 2^5 & \text{otherwise.} \end{cases}$$

Hence we have a sequence of period 2^5 as follows: 0, 15, 14, 13, 12, 11, 10, 9, 8, 23, 22, 20, 19, 18, 17, 16, 31, 30, 29, 28, 27, 26, 25, 24, 7, 6, 5, 4, 3, 2, 1, 0, $\cdots$

Remark 3.5. Example 3.1 is the special case $i = n - 1$ in Theorem 3.3. If $i = 0$, then $x \equiv \bmod 2^0$ for every integer x. Hence $f(x) \equiv x + 1 \bmod 2^n$, which is shown in Example 3.2.

Theorem 3.6. *Let f be a single cycle T-function generated by $a = 2^i - 1$, where $0 < i \leq n - 1$. Then*

$$f(x) = \begin{cases} x + 1 \bmod 2^n & \text{if } x \not\equiv -1 \bmod 2^i \\ x - 2a - 1 \bmod 2^n & \text{if } x \equiv -1 \bmod 2^i. \end{cases}$$

Proof. Let $x = x_{n-1} \cdots x_1 x_0$ and let k be the least nonnegative integer such that $x_k \neq a_k$. If $x \not\equiv -1 \bmod 2^i$, then $k < i$ and

$$[f(x)]_l = \begin{cases} x_l \oplus 1 & \text{if } l \leq k \\ x_l & \text{if } l \geq k + 1. \end{cases}$$

Note that $f(\cdots x_{k+1} 01 \cdots 1) = \cdots x_{k+1} 10 \cdots 0$. Hence $f(x) \equiv x + 1 \bmod 2^n$. Assume that $x \equiv -1 \bmod 2^i$. Then $k \geq i$ or there is no k such that $x_k \neq a_k$. If $k \geq i$, then $[f(x)]_l = \begin{cases} x_l \oplus 1 & \text{if } l \leq k \\ x_l & \text{if } l \geq k+1. \end{cases}$ Note that $f(\cdots x_{k+1} 11 \cdots 1) = \cdots x_{k+1} 00 \cdots 0$ if $k = i$ and $f(\cdots x_{k+1} 10 \cdots 01 \cdots 1) = \cdots x_{k+1} 01 \cdots 10 \cdots 0$ if $k > i$. Hence $f(x) \equiv x - 2^{i+1} + 1 \bmod 2^n$. Also, if there is no k such that $x_k \neq a_k$, then $y_t = x_t \oplus 1$ for all t. Hence $f(x) \equiv x + 2^{n-1} + \cdots 2^{i+1} + 1 \equiv x - 2^{i+1} + 1 \bmod 2^n$. Since $2^{i+1} \equiv 2a + 2 \bmod 2^n$, Theorem 3.6 holds. □

EXAMPLE 3.7. Let $n = 5$ and $i = 1$. Then

$$f(x) = \begin{cases} x + 1 \bmod 2^5 & \text{if } x \equiv 0 \bmod 2 \\ x - 3 \bmod 2^5 & \text{if } x \equiv 1 \bmod 2. \end{cases}$$

Hence we have a sequence of period 2^5 as follows: 0, 1, 30, 31, 28, 29, 26, 27, 24, 25, 22, 23, 20, 21, 18, 19, 16, 17, 14, 15, 12, 13, 10, 11, 8, 9, 6, 7, 4, 5, 2, 3, 0, $\cdots$.

REMARK 3.8. Example 3.2 is the special case $i = n - 1$ in Theorem 3.6. Also, Example 3.1 is the special case $i = 0$ in Theorem 3.6.

THEOREM 3.9. *Let f be a single cycle T-function generated by $a = 2^i$, where $0 \leq i \leq n-2$. Then*

$$f(x) \equiv \begin{cases} x - 1 \ mod\ 2^n & if\ x \not\equiv 0\ mod\ 2^i \\ x + 2a - 1\ mod\ 2^n & if\ x \equiv 0\ mod\ 2^{i+1} \\ x - 2a - 1\ mod\ 2^n & if\ x \equiv 2^i\ mod\ 2^{i+1}. \end{cases}$$

Proof. If $i = 0$, then by the case $i = 1$ in Theorem 3.6 , $f(x) \equiv \begin{cases} x + 1 \bmod 2^n & \text{if } x \equiv 0 \bmod 2 \\ x - 3 \bmod 2^n & \text{if } x \equiv 1 \bmod 2 \end{cases}$, which is a special case $i = 0$ in this theorem. Let $x = x_{n-1} \cdots x_i \cdots x_0$. If $x \not\equiv 0 \bmod 2^i$, then there is the least nonnegative integer $k < i$ such that $x_k \neq a_k$. Note that

$$[f(x)]_l = \begin{cases} 1 \oplus x_l & \text{if } l \leq k \\ x_l & \text{if } l > k. \end{cases}$$

Hence $f(x) \equiv x - 1 \bmod 2^n$. Suppose that $x \equiv 0 \bmod 2^i$. If $x \equiv 0 \bmod 2^{i+1}$, then $[f(x)]_l = \begin{cases} 1 \oplus x_l & \text{if } l \leq i \\ x_l & \text{if } l > i \end{cases}$ and so $f(x) \equiv x + 2^{i+1} - 1 \bmod 2^i$. Suppose $x \equiv 2^i \bmod 2^{i+1}$. Then we have two cases $x_{n-2} \cdots x_0 = a$ and $x_{n-2} \cdots x_0 \neq a$. If $x_{n-2} \cdots x_0 = a$, then $[f(x)]_l = 1 \oplus x_l$ for all l and $f(x) \equiv x - 2^{i+1} - 1 \bmod 2^n$. If $x_{n-2} \cdots x_0 \neq a$, then there is the least nonnegative integer $k > i$ such that $x_k \neq a_k$. Hence $x_i = 0 \neq a_i$ and so $[f(x)]_l = \begin{cases} 1 \oplus x_l & \text{if } l \leq k \\ x_l & \text{if } l > k \end{cases}$. Hence $f(x) \equiv x - 2^{i+1} - 1 \bmod 2^n$. Therefore we have completely proved this theorem. □

EXAMPLE 3.10. Let $n = 5$ and $i = 1$. Then

$$f(x) \equiv \begin{cases} x - 1 \bmod 2^5 & \text{if } x \equiv 1 \bmod 2 \\ x + 3 \bmod 2^5 & \text{if } x \equiv 0 \bmod 2^2 \\ x - 5 \bmod 2^5 & \text{if } x \equiv 2 \bmod 2^2. \end{cases}$$

Hence we have a sequence of period 2^5 as follows: 0, 3, 2, 29, 28, 31, 30, 25, 24, 27, 26, 21, 20, 23, 22, 17, 16, 19, 18, 13, 12, 15, 14, 9, 8, 12, 15, 14, 9, 8, 11, 10, 5, 4, 7, 6, 1, 0, $\cdots$.

THEOREM 3.11. *Let f be a single cycle T-function generated by $a = 2^{i+1} + 2^i$, where $0 \le i \le n-3$. Then*

$$f(x) \equiv \begin{cases} x - 1 \bmod 2^n & \text{if } x \not\equiv 0 \bmod 2^i \\ x - 2a - 1 \bmod 2^n & \text{if } x \equiv a \bmod 2^{i+2} \\ x + 2^{i+1} - 1 \bmod 2^n & \text{otherwise.} \end{cases}$$

Proof. If $i = 0$, then by the case $i = 2$ in Theorem 3.6
$f(x) \equiv \begin{cases} x + 1 \bmod 2^n & \text{if } x \not\equiv 3 \bmod 2^2 \\ x - 7 \bmod 2^n & \text{if } x \equiv 3 \bmod 2^2 \end{cases}$, which is a special case $i = 0$ in this theorem. Let $x = x_{n-1} \cdots x_i \cdots x_0$. If $x \not\equiv 0 \bmod 2^i$, then by Theorem 3.9 $f(x) \equiv x - 1 \bmod 2^n$. Suppose that $x \equiv a \bmod 2^{i+2}$. If $x \not\equiv a \bmod 2^{n-1}$ then there is the least positive integer $l > i + 1$ such that $x_l = 1$. Hence

$$x_k = \begin{cases} x_k \oplus 1 & \text{for all } k \le l \\ x_k & \text{for all } k > l. \end{cases}$$

Hence $f(x) \equiv x - 2a - 1 \bmod 2^n$. If $x \equiv a \bmod 2^{n-1}$, then clearly $f(x) \equiv x - 2a - 1 \bmod 2^n$. Now, it remains to show the case satisfying both $x \equiv a \bmod 2^i$ and $x \not\equiv a \bmod 2^{i+2}$. That is, there are two cases : $x = x_{n-1} \cdots x_{i+2}010 \cdots 0$ and $x = x_{n-1} \cdots x_{i+2}10 \cdots 0$. We can easily get $f(x) \equiv x + 2^{i+1} - 1 \bmod 2^n$. Therefore Theorem 3.11 holds. □

THEOREM 3.12. *Let f be a single cycle T-function generated by $a = 2^{n-1} - 2^i - 1$, where $0 \le i \le n-2$. Then*

$$f(x) \equiv \begin{cases} x + 1 \bmod 2^n & \text{if } x \not\equiv -1 \bmod 2^i \\ x - 2a - 1 \bmod 2^n & \text{if } x \equiv 2^i - 1 \bmod 2^{i+1} \\ x + 2a + 3 \bmod 2^n & \text{if } x \equiv -1 \bmod 2^{i+1}. \end{cases}$$

Proof. If $i = 0$, then by the case $i = 1$ in Theorem 3.3
$f(x) \equiv \begin{cases} x + 3 \bmod 2^n & \text{if } x \equiv 0 \bmod 2 \\ x - 1 \bmod 2^n & \text{otherwise} \end{cases}$, which is a special case $i = 0$ in this theorem. Let $x = x_{n-1} \cdots x_i \cdots x_0$. If $x \not\equiv -1 \bmod 2^i$, then there is the least nonnegative integer $k < i$ such that $x_k \ne a_k$. Note that $[f(x)]_l = \begin{cases} 1 \oplus x_l & \text{if } l \le k \\ x_l & \text{if } l > k. \end{cases}$ Hence $f(x) \equiv x + 1 \bmod 2^n$. Suppose

that $x \equiv -1 \bmod 2^i$. Then we consider two cases $x \equiv 2^i - 1 \bmod 2^{i+1}$ and $x \equiv -1 \bmod 2^{i+1}$. If $x \not\equiv a \bmod 2^{n-1}$, then there is the least nonnegative integer $k \geq i$ such that $x_k \neq a_k$. If $k = i$, then $x_i = 1 \neq a_i$ and so

$$[f(x)]_l = \begin{cases} 1 \oplus x_l & \text{if } l \leq i \\ x_l & \text{if } l > i. \end{cases}$$

Hence $f(x) \equiv x - 2^{i+1} + 1 \bmod 2^n$. If $k > i$, then $x_k = 1 \neq a_k$ and so

$$[f(x)]_l = \begin{cases} 1 \oplus x_l & \text{if } l \leq k \\ x_l & \text{if } l > k. \end{cases}$$

Hence $f(x) \equiv x + 2^{i+1} + 1 \bmod 2^n$. If $x \equiv a \bmod 2^{n-1}$, then $[f(x)]_l \equiv 1 \oplus x_l$, then for all l. Hence $f(x) \equiv x + 2^{i+1} + 1 \bmod 2^n$. □

THEOREM 3.13. *Let f be a single cycle T-function generated by $a = 2^{n-1} - 2^{i+1} - 2^i - 1$, where $0 \leq i \leq n-3$. Then*

$$f(x) \equiv \begin{cases} x + 1 \bmod 2^n & \text{if } x \not\equiv -1 \bmod 2^i \\ x - 2a + 3 \bmod 2^n & \text{if } x \equiv -1 \bmod 2^{i+1} \\ x - 2a - 1 \bmod 2^n & \text{if } x \equiv 2^i - 1 \bmod 2^{i+1}. \end{cases}$$

Proof. If $i = 0$, then $a = 2^{n-1} - 2^2$. Hence by the case $i = 2$ in Theorem 3.3 $f(x) \equiv \begin{cases} x + 7 \bmod 2^n & \text{if } x \equiv 0 \bmod 2^2 \\ x - 1 \bmod 2^n & \text{otherwise} \end{cases}$, which is a special case $i = 0$ in this theorem. Let $x = x_{n-1} \cdots x_i \cdots x_0$. If $x \not\equiv a \bmod 2^{n-1}$, then there is the least nonnegative integer $k \leq n-2$ such that $x_k \neq a_k$. In this case $[f(x)]_l = \begin{cases} 1 \oplus x_l & \text{if } l \leq k \\ x_l & \text{if } l > k. \end{cases}$ If $k \leq i-1$, then $x = x_{n-1} \cdots x_i 101 \cdots 1$ and $f(x) = x_{n-1} \cdots x_i 110 \cdots 0$. Hence $f(x) \equiv x + 1 \bmod 2^n$. If $k = i$, then $x = x_{n-1} \cdots x_{i+1} 11 \cdots 1$ and $f(x) = x_{n-1} \cdots x_{i+1} 000 \cdots 0$. Hence $f(x) = x - 2^{i+1} + 1 \bmod 2^n$. If $k = i+1$, then $x = x_{n-1} \cdots x_{i+2} 101 \cdots 1$ and $f(x) = x_{n-1} \cdots x_{i+2} 010 \cdots 0$. Hence $f(x) \equiv x - 2^{i+1} + 1 \bmod 2^n$. If $k > i+1$, then $x = x_{n-1} \cdots x_{i+2} 001 \cdots 1$ and $f(x) = y_{n-1} \cdots y_{i+2} 110 \cdots 0$, where $y_l = x_l \oplus 1$ for all $l \leq k$ and $y_l = x_l = 1$ for all $l > k$. Hence $f(x) \equiv x + 2^{i+2} + 2^{i+1} + 1 \equiv x - 2a - 1 \bmod 2^n$. □

REMARK 3.14. We get 3 sequences in Example 3.4, Example 3.7 and Example 3.10. Even though finding functions that generate 3 sequences is not hard, compared to the other 2 sequences, it could be difficult to find a function that generates the sequence in Example 3.10. In general it is hard to find a function from a sequence by generated general functions $\alpha_1, \cdots, \alpha_{n-1}$. It is important in stream ciphers to obtain a function that generates a random number sequence generated by the given suitable functions $\alpha_1, \cdots, \alpha_{n-1}$. It is one of the valuable topics which will be studied in future.

References

[1] A. Kilmov, *Applications of T-functions in Cryptography,* Ph.D. Thesis Weizmann Institute Science, 2005.

[2] A. Kilmov and A. Shamir, *Applications of T-functions in Cryptography,* 2005.

[3] A. Kilmov and A. Shamir, *A New Class of Invertible Mappings,* CHES 2002, LNCS 2523, 470-483, 2003.

[4] A. Kilmov and A. Shamir, *Cryptographic Applications of T-functions,* SAC 2003, LNCS 3006, 248-261, 2004.

[5] A. Kilmov and A. Shamir, *New Cryptographic Primitives Based on Multiword T-Functions,* FSE 2004, LNCS 3017, 1-15, 2004.

[6] A. Kilmov and A. Shamir, *New Applications of T-functions in Block Ciphers and Hash Functions,* FSE 2005, LNCS 3557, 18-31, 2005.

[7] M. S. Rhee, *On a characterization of T-function with on cycle property,* J. of the Chungcheong Math. Soc. **21** (2008), no. 2, 259-268.

[8] M. S. Rhee, *On secure binary sequences generated by a function* $f(x) = x + (g(x)^2 \vee C)$ *mod* 2^n, J. of the Chungcheong Math. Soc. **22** (2009), no. 4, 777-789.

*

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