The Single Cycle T-functions

Zhaopeng Dai[1,2] and Zhuojun Liu[1]

[1] Academy of Mathematics and Systems Science, Chinese Academy of Sciences,
China, Beijing, 100190

[2] Graduate University of the Chinese Academy of Sciences, China, Beijing, 100049

Abstract In this paper the single cycle T-functions are studied. Making use of the explicit formulas of sum and product of 2-adic integers, we present the necessary and sufficient conditions on the generalized polynomial $\widetilde{p(x)} = a_0 \overset{+}{\oplus} a_1 x \overset{+}{\oplus} \cdots \overset{+}{\oplus} a_d x^d (\bmod 2^n)$ being a single cycle T-function. Furthermore, for any given generalized polynomial, we can deduce some expressions about its coefficients by which we can determine whether it is single cycle or not.

Key words T-function, single cycle, generalized polynomial

1 Introduction

T-functions, as important classes of cryptographic primitives, have been studied by Anashin([1]-[7]) and also Klimov and Shamir([8]-[12]). Loosely speaking, a T-function is a mapping from an n-bit input to an n-bit output in which each bit i of the output depends only on bits $0, 1, \ldots, i$ of the input. All the logical operations, such as XOR, AND, OR, NOT, and most of the arithmetic operations modulo 2^n, such as addition, multiplication, subtraction, negation, as well as left shift are T-functions, and their compositions are also T-functions([12]). It is well known that T-functions are well-suited for use in the design of secure and efficient stream ciphers, pseudorandom number generators, and so on. For example, Klimov and Shamir proposed in [8] a T-function: $f(x) = x + (x^2 \vee C) (\bmod 2^n)$, where C is a constant integer satisfying $C \equiv 5 \,\text{or}\, 7 (\bmod 2^3)$, used as a pseudorandom number generator. Afterwards, TSC-series stream ciphers ([13],[14],[15]) which are based on T-functions were proposed by Hong et al. as one of the candidates for the ECRYPT Stream Cipher project.

From the point of view of applications, especially in the construction of synchronous stream ciphers, the T-function is expected to have the single cycle

2000 *Mathematics Subject Classification:* 94A60.

This research is supported by National Basic Research Program of China 2011CB302400, National Natural Science Foundation of China (NSFC60821002/F02, 10871106).

Zhaopeng Dai: dzpeng@amss.ac.cn.

Zhuojun Liu: zliu@mmrc.iss.ac.cn.

property, which means that the T-function's repeated application to any initial state goes through all the possible states. To characterize the single cycle property and other cryptographic properties of T-functions, Anashin([7]) developed a very general theory of T-function over p-adic integer rings and applied p-adic analysis to construct wide classes of T-functions with provable cryptographic properties. Meanwhile, Klimov and Shamir introduced the bit-slice analysis method in [10] to study the T-functions. Using of their method, they studied in [12] the generalized polynomials with integral coefficients

$$\widetilde{p(x)} = a_0 \mathbin{\substack{+\\ \oplus}} a_1 x \mathbin{\substack{+\\ \oplus}} \cdots \mathbin{\substack{+\\ \oplus}} a_d x^d \pmod{2^n}$$

as an important class of T-functions and obtained the necessary and sufficient condition that $\widetilde{p(x)}$ is a permutation, while conditions for generating a single cycle have not been stated. In this paper, making use of the bit-slice analysis method and the explicit formulas of sum and product of 2-adic integers in [16], we provide a complete characterization of $\widetilde{p(x)}$ with single cycle.

The remainder of this paper is organized as follows. In Section 2, we give a brief overview of some basic definitions and some related important previously known properties. In Section 3, we discuss the generalized polynomials. Concluding remarks are given in Section 4.

2 Preliminaries

Let $GF(2)$ be the binary field, n an arbitrary nonnegative integer. A word $x \in GF^n(2)$ is the vector $x = ([x]_0, [x]_1, \ldots, [x]_{n-1})$ of length n, where $[x]_i$ denotes its $(i+1)$-st bit; $[x]_0$ is the least significant bit of the word x. Each word can also be interpreted as an integer $x = \sum_{i=0}^{n-1} [x]_i 2^i$ in the residue class ring $\mathbb{Z}/2^n\mathbb{Z}$, with the usual conversion rule: $([x]_0, [x]_1, \ldots, [x]_{n-1}) \longleftrightarrow \sum_{i=0}^{n-1} [x]_i 2^i$. "$\oplus$" denotes the addition in the binary field and "$+$" the addition in the residue class ring $\mathbb{Z}/2^n\mathbb{Z}$. Denote $\mathcal{F}_n$ the set of the Boolean functions of n variables.

Now we give some explicit definitions.

Definition 1 ([8]) A function f from $GF^n(2)$ to $GF^n(2)$ is called a T-function if the i-th bit of the output $[f(x)]_{i-1}$ depends only on the first i bits of the input $[x]_0, \ldots, [x]_{i-1}$

$$\begin{pmatrix} [x]_0 \\ [x]_1 \\ \vdots \\ [x]_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} f_0([x]_0) \\ f_1([x]_0, [x]_1) \\ \vdots \\ f_{n-1}([x]_0, [x]_1, \ldots, [x]_{n-1}) \end{pmatrix}.$$

Definition 2 ([12]) A parameter function is a function

$$g([x]_0, [x]_1, \ldots, [x]_{n-1}; \alpha_0, \alpha_1, \ldots, \alpha_{m-1})$$

whose arguments are split by a semicolon into inputs $[x]_i$ and parameters α_j which do not depend on their inputs.

In this paper, the parameter is always denoted as α.

Definition 3 ([12]) **(Invertible mapping)** A mapping $\varphi : GF^n(2) \longrightarrow GF^n(2)$ is called invertible if $\varphi(x) = \varphi(y)$ if and only if $x = y$.

Definition 4 ([12]) **(A single cycle mapping)** A mapping is called a single cycle mapping if its induced graph is isomorphic to a single cycle.

Obviously, a single cycle mapping is an invertible mapping.

In 2006, Wenying Zhang and Chuankun Wu presented the following characterization of the single cycle T-function modulo 2^n.

Theorem 1 ([17]) Let $f(x) = ([f(x)]_0, [f(x)]_1, \ldots, [f(x)]_{n-1})$ be an invertible T-function over $GF^n(2)$. Then f is a single cycle T-function if and only if its ANF has the following form
$[f(x)]_0 = [x]_0 \oplus 1,$
$[f(x)]_i = [x]_i \oplus [x]_0[x]_1 \cdots [x]_{i-1} \oplus \psi_i([x]_0, \ldots, [x]_{i-1})$ $(*)$
where $\psi_i([x]_0, \ldots, [x]_{i-1}) \in \mathcal{F}_i$ and $deg(\psi_i) < i, i \geq 1$.

We need to state the following lemmas which are used to prove the main results in this paper.

Lemma 1 belongs to the mathematical folklore, thus the proof is omitted.

Lemma 1 Let $\varphi(x) \in \mathcal{F}_n$, then $deg(\varphi(x)) < n$ if and only if

$$\bigoplus_{x \in GF^n(2)} \varphi(x) = 0.$$

Lemma 2 ([16]) Assume that

$$a = \sum_{i=0}^{\infty} a_i 2^i, b = \sum_{i=0}^{\infty} b_i 2^i, a + b = \sum_{i=0}^{\infty} c_i 2^i \in \mathbb{Z}_2,$$

with $a_i, b_i, c_i \in \{0, 1\}$, where $\mathbb{Z}_2$ is the ring of 2-adic integers.

Then we have $c_0 = a_0 + b_0 (\mathrm{mod}\, 2)$, and for $t \geq 1$,

$$c_t = a_t + b_t + \sum_{i=0}^{t-1} a_i b_i \prod_{j=i+1}^{t-1} (a_j + b_j) (\mathrm{mod}\, 2).$$

Define $\theta_t(a,b) = \sum_{i=0}^{t-1} a_i b_i \prod_{j=i+1}^{t-1} (a_j + b_j) (\mathrm{mod}\, 2)$, for $t \geq 1$. In fact, $\theta_t(a,b)$ is the carry of the t-th bit of $a + b$.

Denote $\mathbf{L}_2(t) = \{\underline{l} = (l_1, \ldots, l_k, \ldots, l_t) : \sum_{k=1}^{t} l_k 2^k = 2^t, 0 \leq l_k \leq k+1\}$.

$\tau_l(X_0, X_1, \ldots, X_k)$ denotes the l-th elementary symmetric polynomial of $X_0, X_1, \ldots, X_k$.

Lemma 3 ([16]) Assume that

$$a=\sum_{i=0}^{\infty} a_i 2^i, b=\sum_{i=0}^{\infty} b_i 2^i, ab=\sum_{i=0}^{\infty} e_i 2^i$$

with $a_i, b_i, e_i \in \{0,1\}$. Then $e_0 = a_0 b_0 (\bmod 2)$ and for $t \geq 1$,

$$e_t = \sum_{(l_1,\ldots,l_t)\in \mathbf{L}_2(t)} \prod_{1\leq k\leq t} \tau_{l_k}(a_0 b_k, a_1 b_{k-1}, \ldots, a_k b_0)(\bmod 2).$$

By convention, we let $\Delta_{(l_1,\ldots,l_t)} = \prod_{1\leq k\leq t} \tau_{l_k}(a_0 b_k, a_1 b_{k-1}, \ldots, a_k b_0)$.

3 Generalized Polynomials with Single Cycle

Klimov proposed in [12] the generalized polynomial

$$\widetilde{p(x)} = a_0 \overset{+}{\oplus} a_1 x \overset{+}{\oplus} \cdots \overset{+}{\oplus} a_d x^d (\bmod 2^n) \qquad (**)$$

with integral coefficients where "+" and "$\oplus$" may be used arbitrary. Assume that the operations' order of the generalized polynomial is from left to right. The sufficient and necessary condition on the generalized polynomial being a permutation of the elements in $\mathbb{Z}/2^n\mathbb{Z}$ was presented in [12], while conditions for generating a single cycle have not been stated.

At first, we consider two special cases of the generalized polynomials. One special case $p(x) = a_0 \oplus a_1 x \oplus \cdots \oplus a_d x^d (\bmod 2^n)$ was studied in [19]. The other case is the polynomial functions $p(x) = a_0 + a_1 x + \cdots + a_d x^d (\bmod 2^n)$ which are an important class of functions widely used in many branches of cryptography. The following lemma was proved by several authors using different techniques.

Lemma 4 ([3],[12]) A polynomial $P(x) = \sum_{i=0}^{d} a_i x^i$ has a single cycle modulo any 2^n if and only if it has a single cycle modulo 8.

In [18], Jinsong Wang and Wenfeng Qi gave another proof on the sufficient and necessary condition on the polynomial function being single cycle. That is, $f(x)$ generates a single cycle if and only if a_0, a_1 are odd, $\triangle_1, \triangle_2$ are even, $\triangle_1 + \triangle_2 + 2[a_1]_0 \equiv 0(\bmod 2^2)$, and $\triangle_1 + 2[a_2]_0 + 2[a_1]_1 \equiv 0(\bmod 2^2)$, where $\triangle_1 = a_2 + a_4 + \cdots$, $\triangle_2 = a_3 + a_5 + \cdots$.

Using of our method, we present different conditions that a polynomial function generates a single cycle. Now we will use the lemma cited above to prove the following theorem.

Theorem 2 Suppose the polynomial $P(x) = \sum_{i=0}^{d} a_i x^i (\bmod 2^n)$ is invertible for all $n \in \mathbb{N}$, then $P(x)$ is a single cycle mapping if and only if

(1) $[a_0]_0 = 1$;

(2) $(\bigoplus_{j=1}^{d} [a_j]_1) \oplus (\bigoplus_{j=1}^{d} [a_j]_0 \cdot (\bigoplus_{k=0}^{j-1} [a_k]_0)) = 1$;

(3) $[a_2]_0 \oplus (\bigoplus_{\substack{j=1 \\ j odd}}^{d} [a_j]_0 [a_j]_1) \oplus (\bigoplus_{\substack{j=3 \\ j odd}}^{d} [a_j]_1)$

$$\oplus\bigoplus_{j=1}^{\lfloor\frac{d}{2}\rfloor}((\bigoplus_{\substack{k=1\\ kodd}}^{2j-1}[a_k]_0)\cdot([a_{2j}]_1\oplus[a_{2j}]_0\cdot(\bigoplus_{k=0}^{2j-1}[a_k]_0)))$$
$$\oplus\bigoplus_{j=1}^{\lfloor\frac{d-1}{2}\rfloor}([a_{2j+1}]_1\cdot(\bigoplus_{\substack{k=1\\ kodd}}^{2j-1}[a_k]_0)\oplus[a_{2j+1}]_0\cdot(\bigoplus_{k=0}^{2j}([a_k]_0\oplus[a_k]_1)$$
$$\oplus(\bigoplus_{\substack{k=1\\ kodd}}^{2j-1}[a_k]_0)(\bigoplus_{\substack{k=0\\ keven}}^{2j}[a_k]_0)\oplus\bigoplus_{k=1}^{2j}[a_k]_0\cdot(\bigoplus_{l=0}^{k-1}[a_l]_0)))=0.$$

Proof From Theorem 1, we should check the ANFs of $[P(x)]_i$ whether satisfy $(*)$. From Lemma 4, we only need to check the ANFs of $[P(x)]_0,[P(x)]_1,[P(x)]_2$.

First, $[P(x)]_0=[x]_0\oplus[a_0]_0$.

From Theorem 3.1 in [19] , we know

$$\bigoplus_{j=0}^{d}[a_jx^j]_1=[x]_1\oplus(\bigoplus_{k=1}^{d}[a_k]_1)[x]_0\oplus[a_0]_1.$$

Therefore, we have

$$\begin{aligned}[P(x)]_1&=[a_0]_1\oplus[a_1x]_1\oplus\cdots\oplus[a_dx^d]_1\oplus\theta_1(a_0,a_1x)\oplus\cdots\oplus\theta_1(a_0+\cdots+a_{d-1}x^{d-1},a_dx^d)\\
&=[x]_1\oplus([a_1]_1\oplus\cdots\oplus[a_d]_1)[x]_0\oplus[a_0]_1\oplus([a_0]_0[a_1x]_0\oplus\cdots\\
&\quad\oplus[a_0+\cdots+a_{d-1}x^{d-1}]_0[a_dx^d]_0)\\
&=[x]_1\oplus([a_1]_1\oplus\cdots\oplus[a_d]_1)[x]_0\oplus[a_0]_1\oplus([a_0]_0[a_1]_0\\
&\quad\oplus([a_0]_0\oplus[a_1]_0)[a_2]_0\oplus\cdots\oplus([a_0]_0\oplus[a_1]_0\oplus\cdots\oplus[a_{d-1}]_0)[a_d]_0)[x]_0\\
&=[x]_1\oplus(([a_1]_1\oplus\cdots\oplus[a_d]_1)\oplus([a_0]_0[a_1]_0\oplus([a_0]_0\oplus[a_1]_0)[a_2]_0\oplus\cdots\\
&\quad\oplus([a_0]_0\oplus[a_1]_0\oplus\cdots\oplus[a_{d-1}]_0)[a_d]_0))[x]_0\oplus[a_0]_1;\end{aligned}$$

Now we consider $[P(x)]_2$.

$\theta_2(a_0,a_1x)=[a_0]_0[a_1x]_0([a_0]_1\oplus[a_1x]_1)\oplus[a_0]_1[a_1x]_1=[a_0]_0[a_1]_0[x]_0[x]_1\oplus\alpha$;

For $k=1,2,\ldots,$

$$\begin{aligned}&\theta_2(a_0+\cdots+a_{2k-1}x^{2k-1},a_{2k}x^{2k})\\
=&[a_0+\cdots+a_{2k-1}x^{2k-1}]_0[a_{2k}x^{2k}]_0([a_0+\cdots+a_{2k-1}x^{2k-1}]_1\oplus[a_{2k}x^{2k}]_1)\\
&\oplus[a_0+\cdots+a_{2k-1}x^{2k-1}]_1[a_{2k}x^{2k}]_1\\
=&([a_0]_0\oplus\cdots\oplus[a_{2k-1}x^{2k-1}]_0)[a_{2k}x^{2k}]_0([a_0]_1\oplus\cdots\oplus[a_{2k-1}x^{2k-1}]_1\oplus[a_{2k}x^{2k}]_1\\
&\oplus\theta_0(a_0,a_1x)\oplus\cdots\oplus\theta_0(a_0+\cdots+a_{2k-2}x^{2k-2},a_{2k-1}x^{2k-1}))\\
&\oplus([a_0]_1\oplus\cdots\oplus[a_{2k-1}x^{2k-1}]_1\oplus\theta_0(a_0,a_1x)\oplus\cdots\\
&\oplus\theta_0(a_0+\cdots+a_{2k-2}x^{2k-2},a_{2k-1}x^{2k-1}))[a_{2k}x^{2k}]_1\\
=&(\bigoplus_{\substack{i=1\\ iodd}}^{2k-1}[a_i]_0)([a_{2k}]_1\oplus[a_{2k}]_0(\bigoplus_{i=0}^{2k-1}[a_i]_0))[x]_0[x]_1\oplus\alpha\end{aligned}$$

$$\begin{aligned}&\theta_2(a_0+\cdots+a_{2k}x^{2k},a_{2k+1}x^{2k+1})\\
=&[a_0+\cdots+a_{2k}x^{2k}]_0[a_{2k+1}x^{2k+1}]_0([a_0+\cdots+a_{2k}x^{2k}]_1\oplus[a_{2k+1}x^{2k+1}]_1)\\
&\oplus[a_0+\cdots+a_{2k}x^{2k}]_1[a_{2k+1}x^{2k+1}]_1\\
=&([a_0]_0\oplus\cdots\oplus[a_{2k}x^{2k}]_0)[a_{2k+1}x^{2k+1}]_0([a_0]_1\oplus\cdots\oplus[a_{2k}x^{2k}]_1\oplus[a_{2k+1}x^{2k+1}]_1\\
&\oplus\theta_0(a_0,a_1x)\oplus\cdots\oplus\theta_0(a_0+\cdots+a_{2k-1}x^{2k-1},a_{2k}x^{2k}))\\
&\oplus([a_0]_1\oplus\cdots\oplus[a_{2k}x^{2k}]_1\oplus\theta_0(a_0,a_1x)\oplus\cdots\oplus\theta_0(a_0+\cdots+a_{2k-1}x^{2k-1},a_{2k}x^{2k}))[a_{2k+1}x^{2k+1}]_1\\
=&([a_{2k+1}]_1\cdot(\bigoplus_{\substack{i=1\\ iodd}}^{2k-1}[a_i]_0)\oplus[a_{2k+1}]_0\cdot(\bigoplus_{i=0}^{2k}([a_i]_0\oplus[a_i]_1)\oplus(\bigoplus_{\substack{i=0\\ ieven}}^{2k}[a_i]_0)\cdot(\bigoplus_{\substack{i=0\\ iodd}}^{2k}[a_i]_0)\\
&\oplus\bigoplus_{i=1}^{2k}([a_i]_0(\bigoplus_{l=0}^{i-1}[a_l]_0))))[x]_0[x]_1\oplus\alpha\end{aligned}$$

Then

$$\begin{aligned}
&\theta_2(a_0, a_1x) \oplus \cdots \oplus \theta_2(a_0 + \cdots + a_{d-1}x^{d-1}, a_dx^d)\\
&= ([a_0]_0 \oplus \bigoplus_{k=1}^{\lfloor \frac{d}{2} \rfloor}((\bigoplus_{\substack{i=1\\ i odd}}^{2k-1}[a_i]_0)([a_{2k}]_1 \oplus [a_{2k}]_0(\bigoplus_{i=0}^{2k-1}[a_i]_0)))\\
&\quad \oplus \bigoplus_{k=1}^{\lfloor \frac{d-1}{2} \rfloor}([a_{2k+1}]_1 \cdot (\bigoplus_{\substack{i=1\\ i odd}}^{2k-1}[a_i]_0) \oplus [a_{2k+1}]_0 \cdot (\bigoplus_{i=0}^{2k}([a_i]_0 \oplus [a_i]_1) \oplus (\bigoplus_{\substack{i=0\\ i even}}^{2k}[a_i]_0)\\
&\quad \cdot (\bigoplus_{\substack{i=0\\ i odd}}^{2k}[a_i]_0) \oplus \bigoplus_{i=1}^{2k}([a_i]_0(\bigoplus_{l=0}^{i-1}[a_l]_0)))))[x]_0[x]_1 \oplus \alpha
\end{aligned}$$

From Theorem 3.1 in [19], we know

$$\bigoplus_{j=0}^{d}[a_jx^j]_2 = [x]_2 \oplus ((\bigoplus_{\substack{k=0\\ k odd}}^{d}[a_k]_0[a_k]_1) \oplus (\bigoplus_{\substack{k=3\\ k odd}}^{d}[a_k]_1) \oplus [a_2]_0)[x]_0[x]_1 \oplus \alpha.$$

Finally, we have

$$\begin{aligned}
[P(x)]_2 &= [a_0]_2 \oplus [a_1x]_2 \oplus \cdots \oplus [a_dx^d]_2 \oplus \theta_2(a_0, a_1x) \oplus \cdots \oplus \theta_2(a_0 + \cdots + a_{d-1}x^{d-1}, a_dx^d)\\
&= [x]_2 \oplus ([a_2]_0 \oplus \bigoplus_{\substack{i=0\\ i odd}}^{d}[a_i]_0[a_i]_1 \oplus \bigoplus_{\substack{i=3\\ i odd}}^{d}[a_i]_1)[x]_0[x]_1\\
&\quad \oplus ([a_0]_0 \oplus \bigoplus_{k=1}^{\lfloor \frac{d}{2} \rfloor}((\bigoplus_{\substack{i=0\\ i odd}}^{2k-1}[a_i]_0)([a_{2k}]_1 \oplus [a_{2k}]_0(\bigoplus_{i=0}^{2k-1}[a_i]_0)))\\
&\quad \oplus \bigoplus_{k=1}^{\lfloor \frac{d-1}{2} \rfloor}([a_{2k+1}]_1 \cdot (\bigoplus_{\substack{i=1\\ i odd}}^{2k-1}[a_i]_0) \oplus [a_{2k+1}]_0 \cdot (\bigoplus_{i=0}^{2k}([a_i]_0 \oplus [a_i]_1)\\
&\quad \oplus (\bigoplus_{\substack{i=0\\ i even}}^{2k}[a_i]_0) \cdot (\bigoplus_{\substack{i=0\\ i odd}}^{2k}[a_i]_0) \oplus \bigoplus_{i=1}^{2k}([a_i]_0(\bigoplus_{l=0}^{i-1}[a_l]_0)))))[x]_0[x]_1 \oplus \alpha\\
&= [x]_2 \oplus ([a_2]_0 \oplus \bigoplus_{\substack{i=0\\ i odd}}^{d}[a_i]_0[a_i]_1 \oplus \bigoplus_{\substack{i=3\\ i odd}}^{d}[a_i]_1\\
&\quad \oplus ([a_0]_0 \oplus \bigoplus_{k=1}^{\lfloor \frac{d}{2} \rfloor}((\bigoplus_{\substack{i=0\\ i odd}}^{2k-1}[a_i]_0)([a_{2k}]_1 \oplus [a_{2k}]_0(\bigoplus_{i=0}^{2k-1}[a_i]_0)))\\
&\quad \oplus \bigoplus_{k=1}^{\lfloor \frac{d-1}{2} \rfloor}([a_{2k+1}]_1 \cdot (\bigoplus_{\substack{i=1\\ i odd}}^{2k-1}[a_i]_0) \oplus [a_{2k+1}]_0 \cdot (\bigoplus_{i=0}^{2k}([a_i]_0 \oplus [a_i]_1)\\
&\quad \oplus (\bigoplus_{\substack{i=0\\ i even}}^{2k}[a_i]_0) \cdot (\bigoplus_{\substack{i=0\\ i odd}}^{2k}[a_i]_0) \oplus \bigoplus_{i=1}^{2k}([a_i]_0(\bigoplus_{l=0}^{i-1}[a_l]_0)))))[x]_0[x]_1 \oplus \alpha
\end{aligned}$$

The proof ends. □

The following lemmas will be used in the main theorem of this part.

Lemma 5 ([19]) For $k \geq 1, i \geq 3$, the Boolean function $[ax^{2k}]_i$ doesn't contain the monomial $[x]_0[x]_1 \cdots [x]_{i-1}$.

Lemma 6 ([19]) For $k \geq 1, i \geq 3$, the Boolean function $[ax^{2k+1}]_i$ doesn't contain the monomial $[x]_0[x]_1 \cdots [x]_{i-1}$.

Lemma 7 ([19]) For $k \geq 2, i \geq 1$, the Boolean function $[x^{2k}]_i$ doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_{i-1}$.

Now, we suppose that the generalized polynomial is of the following form:

$$\widetilde{p(x)} = a_0 \oplus \cdots \oplus a_{i_1-1}x^{i_1-1} + a_{i_1}x^{i_1} \oplus \cdots \oplus a_{i_2-1}x^{i_2-1} + a_{i_2}x^{i_2} \oplus \cdots \oplus a_{i_m-1}x^{i_m-1}$$

$$+a_{i_m}x^{i_m} \oplus \cdots \oplus a_d x^d \,(\mathrm{mod}\, 2^n)$$

where $\{i_1, i_2, \ldots, i_m\} \neq \{1, 2, \ldots, d\}, i_1 \geq 1$. That means all ”+” appear between the monomials $a_{i_j-1}x^{i_j-1}$ and $a_{i_j}x^{i_j}$, where $j = 1, 2, \ldots, m$. Other positions are all ”$\oplus$”. Denote

$$f_j = a_0 \oplus \cdots \oplus a_{i_1-1}x^{i_1-1} + a_{i_1}x^{i_1} \oplus \cdots \oplus a_{i_2-1}x^{i_2-1} + a_{i_2}x^{i_2} \oplus \cdots \oplus a_{i_j-1}x^{i_j-1}$$

Theorem 3 Suppose the polynomial

$$\widetilde{p(x)} = a_0 \underset{\oplus}{+} a_1 x \underset{\oplus}{+} \cdots \underset{\oplus}{+} a_d x^d \,(\mathrm{mod}\, 2^n)$$

is invertible for any $n \in \mathbb{N}$ and there are l odd numbers in the set $\{i_1, i_2, \ldots, i_m\}$, where $\{i_1, i_2, \ldots, i_m\} \neq \{1, 2, \ldots, d\}, i_1 \geq 1$. Then $\widetilde{p(x)}(\mathrm{mod}\, 2^n)$ is a single cycle function for any n if and only if $\widetilde{p(x)}(\mathrm{mod}\, 2^{5+2^l})$ is a single cycle function.

Proof Similarly to the proof of Theorem 2, we look into the ANFs of $[\widetilde{p(x)}]_i$.

First, $[\widetilde{p(x)}]_0 = [x]_0 \oplus [a_0]_0$, $[\widetilde{p(x)}]_i = (\bigoplus_{j=0}^{d}[a_j x^j]_i) \oplus (\bigoplus_{j=1}^{m} \theta_i(f_j, a_{i_j}x^{i_j}))$.

From Theorem 3.1 in [19] , we know

$$\bigoplus_{j=0}^{d}[a_j x^j]_1 = [x]_1 \oplus (\bigoplus_{k=1}^{d}[a_k]_1)[x]_0 \oplus [a_0]_1,$$

$$\bigoplus_{j=0}^{d}[a_j x^j]_2 = [x]_2 \oplus ((\bigoplus_{\substack{k=0\\ kodd}}^{d}[a_k]_0[a_k]_1) \oplus (\bigoplus_{\substack{k=3\\ kodd}}^{d}[a_k]_1) \oplus [a_2]_0)[x]_0[x]_1 \oplus \alpha.$$

For $3 \leq i \leq n-1$,

$$\bigoplus_{j=0}^{d}[a_j x^j]_i = [x]_i \oplus [a_1]_1[x]_0[x]_1 \cdots [x]_{i-1} \oplus \alpha.$$

Therefore, for $i \geq 3$, the coefficients of the monomial $[x]_0[x]_1 \cdots [x]_{i-1}$ in $\bigoplus_{j=0}^{d}[a_j x^j]_i$ are the same.

Now, we look into the coefficients of $[x]_0[x]_1 \cdots [x]_{i-1}$ in $\bigoplus_{j=1}^{m} \theta_i(f_j, a_{i_j}x^{i_j})$. First, consider $\theta_i(a_0 \oplus \cdots \oplus a_k x^k, a_{k+1}x^{k+1})$. Since the following computations are easy to carry out, we omit the details.

(**I**) If k is odd.

When $k = 1$,

$$\theta_1(a_0 \oplus a_1 x, a_2 x^2) = ([a_0]_0 \oplus [a_1]_0)[a_2]_0[x]_0,$$

$$\theta_2(a_0 \oplus a_1 x, a_2 x^2) = ([a_2]_1 \oplus ([a_0]_0 \oplus [a_1]_0)[a_2]_0)[x]_0[x]_1.$$

For $i \geq 3$,

$$\theta_i(a_0 \oplus a_1x, a_2x^2) = ([a_2]_1 \oplus [a_0]_0[a_2]_0)[x]_0[x]_1 \cdots [x]_{i-1} \oplus \alpha.$$

When $k \geq 3$,

$$\theta_1(a_0 \oplus \cdots \oplus a_kx^k, a_{k+1}x^{k+1}) = (\bigoplus_{j=0}^{k}[a_j]_0)[a_{k+1}]_0[x]_0,$$

For $i \geq 2$,

$$\theta_i(a_0 \oplus \cdots \oplus a_kx^k, a_{k+1}x^{k+1}) = (\bigoplus_{\substack{j=0\\ j\,odd}}^{k}[a_j]_0)([a_{k+1}]_1 \oplus (1 \oplus \bigoplus_{\substack{j=0\\ j\,even}}^{k}[a_j]_0)[a_{k+1}]_0)[x]_0[x]_1 \cdots [x]_{i-1} \oplus \alpha.$$

(**II**) If k is even.
When $k = 0$, $\theta_1(a_0, a_1x) = [a_0]_0[x]_0$.
For $i \geq 2$, $\theta_i(a_0, a_1x) = [a_0]_0[x]_0[x]_1 \cdots [x]_{i-1} \oplus \alpha$.
When $k = 2$,

$$\theta_1(a_0 \oplus a_1x \oplus a_2x^2, a_3x^3) = ([a_0]_0 \oplus [a_1]_0 \oplus [a_2]_0)[a_3]_0[x]_0,$$

$$\theta_2(a_0 \oplus a_1x \oplus a_2x^2, a_3x^3) = ([a_3]_1 \oplus (1 \oplus [a_0]_1 \oplus [a_1]_1 \oplus [a_2]_1)[a_3]_0)[x]_0[x]_1 \oplus \alpha,$$

$$\theta_3(a_0 \oplus a_1x \oplus a_2x^2, a_3x^3) = [a_3]_0([a_1]_1 \oplus [a_3]_1)[x]_0[x]_1[x]_2 \oplus \alpha.$$

For $i \geq 4$,

$$\theta_i(a_0 \oplus a_1x \oplus a_2x^2, a_3x^3) = 0.$$

When $k \geq 4$,

$$\theta_1(a_0 \oplus \cdots \oplus a_kx^k, a_{k+1}x^{k+1}) = (\bigoplus_{j=0}^{k}[a_j]_0)[a_{k+1}]_0[x]_0,$$

$$\begin{aligned}\theta_2(a_0 \oplus \cdots \oplus a_kx^k, a_{k+1}x^{k+1}) = &((\bigoplus_{\substack{j=0\\ j\,odd}}^{k}[a_j]_0)([a_{k+1}]_1 \oplus (1 \oplus \bigoplus_{\substack{j=0\\ j\,even}}^{k}[a_j]_0)[a_{k+1}]_0)\\ &\oplus((\bigoplus_{\substack{j=0\\ j\,even}}^{k}[a_j]_0) \oplus (\bigoplus_{j=0}^{k}[a_j]_1))[a_{k+1}]_0)[x]_0[x]_1 \oplus \alpha,\end{aligned}$$

$$\begin{aligned}\theta_3(a_0 \oplus \cdots \oplus a_kx^k, a_{k+1}x^{k+1}) = &((\bigoplus_{\substack{j=0\\ j\,odd}}^{k+1}[a_j]_1) \oplus (\bigoplus_{\substack{j=3\\ j\,odd}}^{k}[a_j]_0)((\bigoplus_{j=0}^{k+1}[a_j]_1) \oplus (\bigoplus_{\substack{j=0\\ j\,even}}^{k}[a_j]_0)))\\ &\cdot[a_{k+1}]_0[x]_0[x]_1[x]_2 \oplus \alpha.\end{aligned}$$

Now, we will show that for all $i \geq 4$, the coefficients of the monomial $[x]_0[x]_1 \cdots [x]_{i-1}$ in $\theta_i(a_0 \oplus \cdots \oplus a_kx^k, a_{k+1}x^{k+1})$ are the same.

Claim 1 For $l \geq 1, i \geq 1$, $[x^{2l+1}]_i$ doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_i$.

Proof $\forall l \geq 1, i \geq 1, [x^{2l+1}]_i = [x^{2l}]_i[x]_0 \oplus \cdots \oplus [x^{2l}]_0[x]_i \oplus \delta_i(x^{2l}, x)$, the monomial of $[x^{2l+1}]_i$ which contains the factor $[x]_i$ is $[x]_0[x]_i$, so $[x^{2l+1}]_i$ doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_i$. □

Claim 2 For $l \geq 0, i \geq 1$, $[x^{2l+1}]_i$ doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_{i-1}$.

Proof
$[x^{2l+1}]_i = [x^{2l} \cdot x]_i$

$$= \sum_{(l_1,\ldots,l_i) \in \mathbf{L}_2(i)} \prod_{1 \leq k \leq i} \tau_{l_k}([x^{2l}]_0[x]_k, [x^{2l}]_1[x]_{k-1}, \ldots, [x^{2l}]_k[x]_0) (\bmod 2)$$

If $l_{i-1} = l_i = 0$, then for all $(l_1, \ldots, l_{i-2}, 0, 0) \in \mathbf{L}_2(i)$,

$$\Delta_{(l_1,\ldots,l_{i-2},0,0)} = \prod_{1 \leq k \leq i-2} \tau_{l_k}([x^{2l}]_0[x]_k, [x^{2l}]_1[x]_{k-1}, \ldots, [x^{2l}]_k[x]_0) (\bmod 2)$$

doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_{i-1}$.
If $l_i = 1$, then

$$\Delta_{(0,\ldots,0,1)} = \tau_{l_i}([x^{2l}]_0[x]_i, [x^{2l}]_1[x]_{i-1}, \ldots, [x^{2l}]_i[x]_0)$$
$$= [x^{2l}]_0[x]_i \oplus [x^{2l}]_1[x]_{i-1} \oplus \cdots \oplus [x^{2l}]_i[x]_0$$

doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_{i-1}$.
If $l_i = 0, l_{i-1} = 2$, then

$$\Delta_{(0,\ldots,0,2,0)} = \tau_2([x^{2l}]_0[x]_{i-1}, [x^{2l}]_1[x]_{i-2}, \ldots, [x^{2l}]_{i-1}[x]_0)$$

Since the monomials which contain the factor $[x]_{i-1}$ contain the factor $[x]_0$, $\Delta_{(0,\ldots,0,2,0)}$ doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_{i-1}$.
If $l_i = 0, l_{i-1} = 1$, we consider the vectors $(l_1, \ldots, l_{i-2}, 1, 0) \in \mathbf{L}_2(i)$.

$$\Delta_{(l_1,\ldots,l_{i-2},1,0)} = \prod_{1 \leq k \leq i-1} \tau_{l_k}([x^{2l}]_0[x]_k, [x^{2l}]_1[x]_{k-1}, \ldots, [x^{2l}]_k[x]_0)$$
$$= \tau_1([x^{2l}]_0[x]_{i-1}, [x^{2l}]_1[x]_{i-2}, \ldots, [x^{2l}]_{i-1}[x]_0)$$
$$\cdot \prod_{1 \leq k \leq i-2} \tau_{l_k}([x^{2l}]_0[x]_k, [x^{2l}]_1[x]_{k-1}, \ldots, [x^{2l}]_k[x]_0)$$

Since the monomials which contain the factor $[x]_{i-1}$ contain the factor $[x]_0$, $\Delta_{(l_1,\ldots,l_{i-2},1,0)}$ doesn't contain the monomial $[x]_1[x]_2 \cdots [x]_{i-1}$. □

Claim 3 For $k \geq 1, i \geq 3$, $[ax^k]_i$ doesn't contain the monomial $[x]_0[x]_1 \cdots [x]_{i-1}$.

Proof This follows directly from Lemma 5 and Lemma 6. □

Furthermore, we have the following proposition.

Claim 4 For $k \geq 3, i \geq 2$, $[ax^k]_i$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$.

Proof If $k = 2l$ is even,

$$[ax^{2l}]_i = [a]_i[x^{2l}]_0 \oplus \cdots \oplus [a]_0[x^{2l}]_i \oplus \delta_i(a, x^{2l}).$$

From Lemma 7, for any $l \geq 2, i \geq 2, [x^{2l}]_i$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$. That means $[ax^{2l}]_i$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$.

If $k = 2l+1$ is odd, then

$$[ax^{2l+1}]_i = \sum_{(l_1,\ldots,l_i)\in\mathbf{L}_2(i)} \prod_{1\leq k\leq i} \tau_{l_k}([a]_0[x^{2l+1}]_k, [a]_1[x^{2l+1}]_{k-1}, \ldots, [a]_k[x^{2l+1}]_0) (\bmod 2).$$

If $l_{i-1} = l_i = 0$, then for any $(l_1, \ldots, l_{i-2}, 0, 0) \in \mathbf{L}_2(i)$, $\Delta_{(l_1,\ldots,l_{i-2},0,0)}$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$.

If $l_i = 1$, then

$$\begin{aligned}\Delta_{(0,\ldots,0,1)} &= \tau_{l_i}([a]_0[x^{2l+1}]_i, [a]_1[x^{2l+1}]_{i-1}, \ldots, [a]_i[x^{2l+1}]_0) \\ &= [a]_0[x^{2l+1}]_i \oplus [a]_1[x^{2l+1}]_{i-1} \oplus \cdots \oplus [a]_i[x^{2l+1}]_0\end{aligned}$$

From Claim 1, $[x^{2l+1}]_{i-1}$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$. From Claim 2, $[x^{2l+1}]_i$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$, then $\Delta_{(0,\ldots,0,1)}$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$.

If $l_i = 0, l_{i-1} = 2$, then

$$\Delta_{(0,\ldots,0,2,0)} = \tau_2([a]_0[x^{2l+1}]_{i-1}, [a]_1[x^{2l+1}]_{i-2}, \ldots, [a]_{i-1}[x^{2l+1}]_0)$$

Since the monomials of $[x^{2l+1}]_{i-1}$ which contain the factor $[x]_{i-1}$ contain the factor $[x]_0$, $\Delta_{(0,\ldots,0,2,0)}$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$.

If $l_i = 0, l_{i-1} = 1$,

$$\begin{aligned}\Delta_{(l_1,\ldots,l_{i-2},1,0)} &= \prod_{1\leq k\leq i-1} \tau_{l_k}([a]_0[x^{2l+1}]_k, [a]_1[x^{2l+1}]_{k-1}, \ldots, [a]_k[x^{2l+1}]_0) \\ &= \tau_1([a]_0[x^{2l+1}]_{i-1}, [a]_1[x^{2l+1}]_{i-2}, \ldots, [a]_{i-1}[x^{2l+1}]_0) \\ &\quad \prod_{1\leq k\leq i-2} \tau_{l_k}([a]_0[x^{2l+1}]_k, [a]_1[x^{2l+1}]_{k-1}, \ldots, [a]_k[x^{2l+1}]_0)\end{aligned}$$

Since the monomials of $[x^{2l+1}]_{i-1}$ which contain the factor $[x]_{i-1}$ contain the factor $[x]_0$, $\Delta_{(l_1,\ldots,l_{i-2},1,0)}$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$.

Therefore, $[ax^{2l+1}]_i$ doesn't contain the monomial $[x]_1[x]_2\cdots[x]_{i-1}$. □

From Claim 3 and Claim 4, we know that for any $k \geq 3, i \geq 3, [ax^k]_i$ doesn't contain the monomial $[x]_0[x]_1\cdots[x]_{i-1}$ and $[x]_1[x]_2\cdots[x]_{i-1}$. Then

$$\sum_{j=3}^{i-1}[a_0\oplus\cdots\oplus a_kx^k]_i[a_{k+1}x^{k+1}]_i\prod_{l=j+1}^{i-1}([a_0\oplus\cdots\oplus a_kx^k]_j\oplus[a_{k+1}x^{k+1}]_j)$$

doesn't contain the monomial $[x]_0[x]_1\cdots[x]_{i-1}$.

Therefore, for $i\geq 4$, the coefficients of $[x]_0[x]_1\cdots[x]_{i-1}$ in $\theta_i(a_0\oplus\cdots\oplus a_kx^k, a_{k+1}x^{k+1})$ are the same.

Now, we consider $\theta_i(f_k, a_{i_k}x^{i_k})\,(k\geq 2)$.

(**I**) If i_k is even.

If $i_k\geq 4$,

$$\theta_1(f_k,a_{i_k}x^{i_k})=[f_k]_0[a_{i_k}x^{i_k}]_0=(\bigoplus_{j=0}^{i_k-1}[a_j]_0)[a_{i_k}]_0[x]_0,$$

For any $l\geq 2$,

$$\theta_l(f_k,a_{i_k}x^{i_k})=(\bigoplus_{\substack{j=0\\ j\,odd}}^{i_k}[a_j]_0)([a_{i_k}]_1\oplus(1\oplus\bigoplus_{\substack{j=0\\ j\,even}}^{i_k-2}[a_j]_0)[a_{i_k}]_0)[x]_0[x]_1\cdots[x]_{l-1}\oplus\alpha.$$

(**II**) If i_k is odd.

Let $k=2$.

Since

$$[f_2]_j[a_{i_2}x^{i_2}]_j=([a_0]_j\oplus[a_1x]_j\oplus\cdots\oplus[a_{i_2-1}x^{i_2-1}]_j\oplus\theta_j(f_1,a_{i_1}x^{i_1}))([a_{i_2}]_0[x]_0[x]_j\oplus\alpha),$$

it follows that the monomial $[x]_0[x]_1\cdots[x]_j$ only appears in $[a_{i_2}]_0[x]_0[x]_j\theta_j(f_1,a_{i_1}x^{i_1})$.

For the same reason, considering $[f_2]_{j+1}[a_{i_2}x^{i_2}]_{j+1}$, the monomial $[x]_0[x]_1\cdots[x]_{j+1}$ only appears in $[a_{i_2}]_0[x]_0[x]_{j+1}\theta_{j+1}(f_1,a_{i_1}x^{i_1})$.

Since, for $i\geq 4$, the coefficients of $[x]_0[x]_1\cdots[x]_{i-1}$ in $\theta_i(a_0\oplus\cdots\oplus a_kx^k, a_{k+1}x^{k+1})$ are the same, it follows that, for all $j\geq 4$, the coefficient of $[x]_0[x]_1\cdots[x]_j$ in $[f_2]_j[a_{i_2}x^{i_2}]_j$ is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+1}$ in $[f_2]_{j+1}[a_{i_2}x^{i_2}]_{j+1}$.

It is easy to see

$$\Lambda=[f_2]_{j-1}[a_{i_2}x^{i_2}]_{j-1}([f_2]_j\oplus[a_{i_2}x^{i_2}]_j)([f_2]_{j+1}\oplus[a_{i_2}x^{i_2}]_{j+1})$$
$$\oplus[f_2]_j[a_{i_2}x^{i_2}]_j([f_2]_{j+1}\oplus[a_{i_2}x^{i_2}]_{j+1})$$

doesn't contain the monomial $[x]_0[x]_1\cdots[x]_{j+1}$.

Obviously, the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in

$$\sum_{l=0}^{j-2}[f_2]_l[a_{i_2}x^{i_2}]_l\prod_{t=l+1}^{j-1}([f_2]_t\oplus[a_{i_2}x^{i_2}]_t)$$

is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+1}$ in

$$\sum_{l=0}^{j-2}[f_2]_l[a_{i_2}x^{i_2}]_l\prod_{t=l+1}^{j+1}([f_2]_t\oplus[a_{i_2}x^{i_2}]_t)$$

Thus, the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in

$$\theta_j(f_2,a_{i_2}x^{i_2})=\sum_{l=0}^{j-1}[f_2]_l[a_{i_2}x^{i_2}]_l\prod_{t=l+1}^{j-1}([f_2]_t\oplus[a_{i_2}x^{i_2}]_t)$$

is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+1}$ in

$$\theta_{j+2}(f_2,a_{i_2}x^{i_2})=\sum_{l=0}^{j+1}[f_2]_l[a_{i_2}x^{i_2}]_l\prod_{t=l+1}^{j+1}([f_2]_t\oplus[a_{i_2}x^{i_2}]_t).$$

Claim 5 If there are $l\leq(k-2)$ odd numbers in the set $\{i_2,i_3,\ldots,i_{k-1}\}$, for $k\geq 3$, then the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in $\theta_j(f_k,a_{i_k}x^{i_k})$ is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+2^{l+1}-1}$ in $\theta_{j+2^{l+1}}(f_k,a_{i_k}x^{i_k})$.

Proof The claim is shown by induction on k.

Let $k=3$.

Similarly to the case of $k=2$, we can show that:

If $i_2\geq 4$ is even, the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in $\theta_j(f_3,a_{i_3}x^{i_3})$ is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+1}$ in $\theta_{j+2}(f_3,a_{i_3}x^{i_3})$.

If $i_2\geq 4$ is odd, the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in $\theta_j(f_3,a_{i_3}x^{i_3})$ is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+1}$ in $\theta_{j+2^2}(f_3,a_{i_3}x^{i_3})$.

Suppose that the proposition holds for all $l\leq k$.

Now we suppose that there are $m\leq(k-1)$ odd numbers in the set $\{i_2,\ldots,i_k\}$. We will show that the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in $\theta_j(f_{k+1},a_{i_{(k+1)}}x^{i_{(k+1)}})$ is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+2^{m+1}-1}$ in $\theta_{j+2^{m+1}}(f_{k+1},a_{i_{(k+1)}}x^{i_{(k+1)}})$.

Similarly to the case of $k=2$, we will divide

$$\theta_j(f_{k+1},a_{i_{(k+1)}}x^{i_{(k+1)}})\text{ and }\theta_{j+2^{m+1}}(f_{k+1},a_{i_{(k+1)}}x^{i_{(k+1)}})$$

into three parts to discuss.

Firstly, since

$$[f_{k+1}]_{j-1}[a_{i_{(k+1)}}x^{i_{(k+1)}}]_{j-1}=(\bigoplus_{l=0}^{i_{(k+1)}-1}[a_lx^l]_{j-1}\oplus\bigoplus_{l=1}^{k}\theta_{j-1}(f_l,a_{i_l}x^{i_l}))([a_{i_{(k+1)}}]_0[x]_0[x]_{j-1}\oplus\alpha),$$

by the induction hypothesis, it is easy to see that

$$\bigoplus_{l=1}^{k}\theta_{j-1}(f_l,a_{i_l}x^{i_l})=(\bigoplus_{\substack{l=1\\ l\,even}}^{k}\theta_{j-1}(f_l,a_{i_l}x^{i_l}))\oplus(\bigoplus_{\substack{l=1\\ l\,odd}}^{k}\theta_{j+2^{m+1}-1}(f_l,a_{i_l}x^{i_l}))$$

$$= \bigoplus_{l=1}^{k} \theta_{j+2^{m+1}-1}(f_l, a_{i_l}x^{i_l}),$$

then the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in $[f_{k+1}]_{j-1}[a_{i_{(k+1)}}x^{i_{(k+1)}}]_{j-1}$ is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+2^{m+1}-1}$ in $[f_{k+1}]_{j+2^{m+1}-1}[a_{i_{(k+1)}}x^{i_{(k+1)}}]_{j+2^{m+1}-1}$.

Secondly,

$$\sum_{l=j-1}^{j+2^{m+1}-2} [f_{k+1}]_l[a_{i_{(k+1)}}x^{i_{(k+1)}}]_l \prod_{t=l+1}^{j+2^{m+1}-1} ([f_{k+1}]_t \oplus [a_{i_{(k+1)}}x^{i_{(k+1)}}]_t)$$

doesn't contain the monomial $[x]_0[x]_1\cdots[x]_{j+2^{m+1}-1}$.

Finally, we can check that the coefficient of $[x]_0[x]_1\cdots[x]_{j-1}$ in

$$\sum_{l=0}^{j-2} [f_{k+1}]_l[a_{i_{k+1}}x^{i_{k+1}}]_l \prod_{t=l+1}^{j-1} ([f_{k+1}]_t \oplus [a_{i_{(k+1)}}x^{i_{(k+1)}}]_t)$$

is equal to the coefficient of $[x]_0[x]_1\cdots[x]_{j+2^{m+1}-1}$ in

$$\sum_{l=0}^{j-2} [f_{k+1}]_l[a_{i_{(k+1)}}x^{i_{(k+1)}}]_l \prod_{t=l+1}^{j+2^{m+1}-1} ([f_{k+1}]_t \oplus [a_{i_{(k+1)}}x^{i_{(k+1)}}]_t).$$

The claim holds and the proof ends. □

Remark In the above theorem, the generalized polynomials $(**)$ are studied in general and the condition for generating a single cycle is presented. In practice, if we treat the coefficients as symbols, then there are 2^d different forms of generalized polynomials, for we have two operations "$+$" and "$\oplus$" to choose between the adjacent monomials. When we consider the concrete case of the generalized polynomial of which the "$+$" and "$\oplus$" appear between the monomials are fixed, we can gain more explicit conditions on the generalized polynomial being single-cycle. Firstly, from Theorem 3, it is easy to determine the number l. Then, we only need to check the ANFs of $[\widetilde{p(x)}]_i$, for $0 \le i \le (4+2^l)$, according to $(*)$ in Theorem 1. Furthermore, using of the formulas of sum and product of 2-adic integers, we can present a more explicit characterization of the coefficients of the single cycle generalized polynomials, just like Theorem 2 above and Theorem 3.1 in [19].

Let us consider a simple case of the generalized polynomial $\widetilde{p(x)} = a_0 + a_1x \oplus a_2x^2 \pmod{2^n}$.

From Theorem 5.3 in [12], we know that $\widetilde{p(x)} \pmod{2^n}$ is invertible for any $n \in \mathbb{N}$ if and only if $[a_1]_0 = 1, [a_2]_0 = 0$.

Moreover, we have the following proposition.

Proposition 1 $\widetilde{p(x)} = a_0 + a_1x \oplus a_2x^2 \pmod{2^n}$ is single cycle for any $n \in \mathbb{N}$ if and only if $[a_0]_0 = [a_1]_0 = 1, [a_1]_1 = [a_2]_0 = [a_2]_1 = 0$.

Proof From Theorem 3, we have $l=1$, thus $\forall n \in \mathbb{N}$, $\widetilde{p(x)}\,(\bmod 2^n)$ is single cycle if and only if $\widetilde{p(x)}\,(\bmod 2^7)$ is single cycle. Therefore, we only need to check the ANFs of $[\widetilde{p(x)}]_i, i=0,1,\ldots,6$.

First, for $i \geq 1$, $\theta_i(a_0, a_1x)$ does not contain the term $[x]_i$, then we consider the coefficient of the term $[x]_0[x]_1\cdots[x]_{i-1}$ in $\theta_i(a_0,a_1x)$.

Since

$$\begin{aligned}\theta_i(a_0,a_1x) = [a_0]_0[a_1x]_0([a_0]_1\oplus[a_1x]_1)([a_0]_2\oplus[a_1x]_2)\cdots([a_0]_{i-1}\oplus[a_1x]_{i-1})\\ \oplus[a_0]_1[a_1x]_1([a_0]_2\oplus[a_1x]_2)\cdots([a_0]_{i-1}\oplus[a_1x]_{i-1})\\ \oplus\cdots\oplus[a_0]_{i-1}[a_1x]_{i-1},\end{aligned}$$

it is easy to know that the monomial $[x]_0[x]_1\cdots[x]_{i-1}$ is only contained in

$$[a_0]_0[a_1x]_0([a_0]_1\oplus[a_1x]_1)([a_0]_2\oplus[a_1x]_2)\cdots([a_0]_{i-1}\oplus[a_1x]_{i-1})$$

and the coefficient is $[a_0]_0$.

From Theorem 3.1 in [19], we have
$[a_0]_0\oplus[a_1x]_0\oplus[a_2x^2]_0=[x]_0\oplus[a_0]_0$,
$[a_0]_1\oplus[a_1x]_1\oplus[a_2x^2]_1=[x]_1\oplus([a_1]_1\oplus[a_2]_1)[x]_0\oplus[a_0]_1$,
$[a_0]_2\oplus[a_1x]_2\oplus[a_2x^2]_2=[x]_2\oplus([a_1]_1\oplus[a_2]_0)[x]_0[x]_1\oplus\alpha$,
for $i\geq 3$, $[a_0]_i\oplus[a_1x]_i\oplus[a_2x^2]_i=[x]_i\oplus[a_1]_1[x]_0[x]_1\cdots[x]_{i-1}\oplus\alpha$.
Therefore,

$$[\widetilde{p(x)}]_0=[a_0]_0\oplus[a_1x]_0\oplus[a_2x^2]_0=[x]_0\oplus[a_0]_0,$$

$$[\widetilde{p(x)}]_1=[a_0]_1\oplus[a_1x]_1\oplus[a_2x^2]_1\oplus\theta_1(a_0,a_1x)=[x]_1\oplus([a_0]_0\oplus[a_1]_1\oplus[a_2]_1)[x]_0\oplus[a_0]_1,$$

$$[\widetilde{p(x)}]_2=[a_0]_2\oplus[a_1x]_2\oplus[a_2x^2]_2\oplus\theta_2(a_0,a_1x)=[x]_2\oplus([a_0]_0\oplus[a_1]_1\oplus[a_2]_0)[x]_0[x]_1\oplus\alpha,$$

for $3\leq i\leq 6$,

$$[\widetilde{p(x)}]_i=[a_0]_i\oplus[a_1x]_i\oplus[a_2x^2]_i\oplus\theta_i(a_0,a_1x)=[x]_i\oplus([a_0]_0\oplus[a_1]_1)[x]_0[x]_1\cdots[x]_{i-1}\oplus\alpha.$$

From Theorem 1, the result follows. □

Example 1 Since $[5]_0=[9]_0=1,[9]_1=[4]_0=[4]_1=0$, from Proposition 1, $\widetilde{p(x)}=5+9x\oplus 4x^2\,(\bmod 2^n)$ is a single cycle function for any $n\in\mathbb{N}$. Its cycle structure over $\mathbb{Z}/2^2\mathbb{Z}$ is $0\to1\to2\to3\to0$.

Example 2 Since $[6]_0\neq1,[3]_1\neq0$, from the above result, we know that $\widetilde{p(x)}=6+3x\oplus 4x^2\,(\bmod 2^n)$ is not a single cycle function for some n. The cycle structure over $\mathbb{Z}/2^3\mathbb{Z}$ is $0\to6\to0$, $1\to5\to1$, $2\to4\to2$, $3\to3$, $7\to7$.

4 Conclusion

In this paper, we have developed the bit-slice analysis of T-functions proposed by Klimov and Shamir in depth. By means of the formulas of sum and product of 2-adic integers, we gain a more explicit characterization of the single cycle T-function. In particular, we study a new class of single cycle T-functions which are called the generalized polynomials and present the necessary and sufficient conditions that the generalized polynomials are single cycle functions.

References

1. V.Anashin, Uniformly distributed sequences of p-adic integers, Math. Notes 55, 1994, 109-133.
2. V.Anashin, Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers. J. Math. Sci. 1998, 89, 1355-1390.
3. V.Anashin, Uniformly distributed sequences of p-adic integers, II. Discrete Math. Appl. 2002, 12, 527-590.
4. V.Anashin, Pseudorandom number generation by p-adic ergodic transformations, arXiv: Cryptography and Security, 2004. http://arxiv.org/abs/cs/0401030/.
5. V.Anashin, Non-Archimedean analysis, T-functions, and cryptography, arXiv: Cryptography and Security, 2006. http://arxiv.org/abs/cs/0612038/.
6. V.Anashin, Wreath products in stream cipher design, arXiv: Cryptography and Security, 2006. http://arxiv.org/abs/cs/0602012/.
7. Vladmir Anashin and Andrei Khrennikov. Applied Algebraic Dynamics. de Gruyter Expositions in Mathematics, vol. 49, Walter de Gruyter, Berlin-New York, 2009.
8. A. Klimov and A.Shamir, A New Class of Invertible Mappings, Workshop on Cryptographic Hardware and Embedded Systems 2002, Lecture Notes in Computer Science, 2003, vol.2523: 470-483.
9. A. Klimov and A.Shamir, Cryptographic Applications of T-functions, Selected Areas in Cryptography(SAC)2003, Lecture Notes in Computer Science, 2004, vol.3006: 248-261.
10. A. Klimov and A.Shamir, New Cryptographic Primitives Based on Multiword T-functions, Fast Software Encryption 2004, Lecture Notes in Computer Science, 2004, vol.3017: 1-15.
11. A. Klimov and A.Shamir, New Applications of T-functions in Block Ciphers and Hash Functions, Fast Software Encryption 2005, Lecture Notes in Computer Science, 2005, vol.3557: 18-31.
12. A. Klimov, Applications of T-functions in Cryptography, Thesis for the degree of Ph.D., Weizmann Institute of Science, 2005.
13. J.Hong, D.Lee, Y.Yeom and D.han, A New Class of Single Cycle T-functions, Fast Software Encryption 2005, Lecture Notes in Computer Science, 2005, vol.3557: 68-82.
14. J.Hong, D.Lee, Y.Yeom, et al, T-function Based Streamcipher TSC-3, http://www.ecrypt.eu. org/stream/tsc3.html.
15. D.Moon, D.Kwon, D.Han, et al, T-function Based Streamcipher TSC-4, http://www.ecrypt.eu. org/stream/tsc3p2.html.

16. Kejian Xu, Zhaopeng Dai and Zongduo Dai, The formulas of coefficients of sum and product of p-adic integers with applications to Witt vectors, ACTA ARITHMETICA (accepted).
17. Wenying Zhang and Chuan-Kun Wu, The Algebraic Normal Form, Linear Complexity and k-Error Linear Complexity of Single-Cycle T-function, Sequences and Their Applications 2006, Lecture Notes in Computer Science, 2006, vol.4086: 391-401.
18. Jin-Song Wang and Wen-Feng Qi, Linear Equation on Polynomial Single Cycle T-functions, Inscrypt 2007, Lecture Notes in Computer Science, 2008, vol.4990: 256-270.
19. Zhuojun Liu, Zhaopeng Dai and Baofeng Wu, Determination of One Kind of Single Cycle T-function, Journal of Systems Science and Mathematical Sciences(in Chinese), 30(11), (2010,11), 1540-1547.