Number formula and degree level of ergodic polynomial functions over $\mathbb{Z}/2^n\mathbb{Z}$ and generalized result of linear equation on ergodic power-series T-Function

Tao Shi and Dongdai Lin
State Key Laboratory of Information Security,
Institute of Software, Chinese Academy of Sciences,
Beijing 100080, P.R. China

September 15, 2010

Abstract

1 Introduction

The objective of stream ciphers is to expand a short key into a long keystream that is difficult to distinguish from a truly random stream. The encryption is done by XORing the plaintext with the keystream, and it should not be possible to reconstruct the key from the keystream. In many years linear feedback shift registers, LFSRs, have been one of the most important building blocks in keystream generators. The advantage with LFSRs is that they can easily be designed to produce maximum-length streams, and they are fast and easy to implement in hardware. However, the LFSRs have a lot of linear properties, which make them easy to cryptanalyze and break. To make the LFSRs more secure they must be combined with other elements, such as S-boxes or Boolean functions. This complicates and slows down the ciphers in software.

Recently, T-functions are found to be useful tools, which help to realize fast encryption under arithmetic(addition, multiplication) and logical operations. Loosely speaking, a T-function is a map of n-bit words into n-bit words such that each i-th bit of image depends only on low-order bit $0, ..., i$ of the pre-image. From the viewpiont of P-adic Analysis, T-functions are continuous (and often differentiable!) functions with respect to the 2-adic distance. This observation gives a powerful tool to apply 2-adic analysis to construct wide classes of T-functions with provable cryptographic properties (long period, balance, uniform distribution, high linear complexity, etc.); Vladimir Anashin [1], Combine with the kowledge of dynamic system, developed a very general theory of T-function over local fields and P-adic integer rings. In there, T-functions is actually the so called "compatible" functions over $\mathbb{Z}_2$.

In the work [2], Jin-Song Wang and Wen-Feng Qi gived the sufficient and necessary condition that a polynomial function $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_mx^m$ with integer coefficients modulo $2^n(n \geq 3)$ is a single cycle T-function, That is, $f(x)$ generates a single cycle if and only if c_0, c_1 are odd, $\triangle_1, \triangle_2$ are even, $\triangle_1 + \triangle_2 + 2c_{1,1} \equiv 0 \bmod 4$, and $\triangle_1 + 2c_{2,0} + 2c_{1,1} \equiv 0 \bmod 4$, where $\triangle_1 = (c_2+c_4+\cdots), \triangle_2 = (c_3+c_5+\cdots)$. A Linear Equation over the coordinate sequences of sequence $\{x_i\}$generated by iterated the polynomial single cycle T-function, that is,

$$x_{i+2^{j-1},j} = x_{i,j} + x_{i,j-1} + ajA_{i,2} + a(j-1) + b \bmod 2, 3 \leq j \leq n-1 \qquad (1)$$

given $x_0 \in \mathbb{Z}/2^n\mathbb{Z}$, where $x_i = f(x_{i-1}) \bmod 2^n$, $x_{i,j}$be the j-th bit of x_i. $A_{i,2}$ is a sequence of period 4 and a, b are constants determined by the coefficients c_i.

In this paper, using Anashin's general theory, some detail combinatorial result of stirling numbers and Larin's result [6] , we can give the counting formula for the given degree polynomial ergodic(single cycle) T-function. we deduce that Jin-Song Wang and Wen-Feng Qi's result is a special case of ours, and their linear relation on the coordinate sequences generated by single cycle polynomial T-function can be extended to a more general function class. The equation shows that the sequences generated by these T-functions have potential secure problems.

2 Preliminary

Now we will try to state some general result of Anashin's p-adic ergodic theory.

A (discrete) dynamical system is just a triple$(\mathbb{S}, \mu, f)$, where $\mathbb{S}$ is a measurable space endowed with a measure μ, $f : \mathbb{S} \to \mathbb{S}$ is a measurable function; that is, an f-preimage of any measurable subset is a measurable subset. A trajectory of the dynamical system is a sequence

$$x_0, x_1 = f(x_0), ..., x_i = f(x_{i-1}) = f^i(x_0), ...$$

of points of the space $\mathbb{S}$, x_0 is called an initial point of the trajectory. Dynamical system theory study trajectories $x_0, x_1 = f(x_0), ..., x_{i+1} = f(x_i) = f^{i+1}(x_0), ...$;In this case, for each measurable subset $\mathbb{T} \subseteq \mathbb{S}$, if $\mu(f^{-1}(\mathbb{T})) = \mu(\mathbb{T})$, we say f is measure preserving, if for each measurable subsets $\mathbb{T} \subseteq \mathbb{S}$, we also have $f^{-1}(\mathbb{T}) = \mathbb{T}$ holds either $\mu(\mathbb{T}) = 1$,or$\mu(\mathbb{T}) = 0$, we say f is ergodic. we usually deal with dynamical systems on finite sets; for every subset U of A, nature discrete measure is $\mu(U) = \#U \cdot (\#A)^{-1}$. Obviously, the mapping $f : A \to A$ preserves measure μ if and only if it is bijective; that is, f is a permutation on A. Finally, f is ergodic if and only if this permutation has only one cycle, of length $\#A$.In the latter case we say that f is transitive on A.

p is a prime number, $\mathbb{Z}_p$ is the p-adic integer ring of local field $\mathbb{Q}_p$, It is consisted by the elements of the form

$$x = x_0 + x_1p + x_2p^2 + \cdots + x_np^n + \cdots, 0 \leq x_i \leq p-1 \qquad (2)$$

$\mathbb{Z}_p$ is endowed with a non-Archimedean absolute value

$$|x|_p = p^{-ord_p x} \tag{3}$$

$|0|_p = 0$. $ord_p : Z\backslash\{0\} \rightarrow \mathbb{N}_0(\mathbb{N}\cup 0)$is the p-adic valuation. The p-adic absolute value is non-Archimedean, i.e. it not only satisfies the normal axioms absolute value,but also the strong triangle inequality $|x+y| \leq max(|x|,|y|)$, It induces a metric $\rho(x,y) = |x-y|_p$.

Definition 1 *A function $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is called compatible if the congruence $u \equiv v(\bmod p^k)$ implies$f(u) \equiv f(v)(\bmod p^k), k \in \mathbb{N}_0$, for every pair $u, v \in \mathbb{Z}_p$.*

In other words, compatible functions are precisely all those functions that satisfy the uniform 1-Lipschitz condition

$$|f(u) - f(v)|_p \leq |u-v|_p \tag{4}$$

Proposition 1 *.[1] A function $f : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$ is compatible if and only if for every $i = 1, 2, ...$ the i-th coordinate function $\delta_i(f(x_1, ..., x_n))$ does not depend on $\delta_{i+k}(x_s)$, for all $s = 1, 2, ..., n$ and $k = 1, 2, ...\delta_i(x)$ means the i-th coordinate of p-adic expansion of x.*

So, T-function is actually the compatible functions over $\mathbb{Z}_2$. From the inequality (4), we kown that all T-function are continue over 2-adic metric. We can describe all p-adic continue functions using Mahler basis, i.e.

Theorem 1 *.[3] W.H.Schikhof Functions $\binom{x}{0}$,$\binom{x}{1}$, $\binom{x}{2}$, . . .form a base of continue function space $C(\mathbb{Z}_p, \mathbb{Q}_p)$, i.e. for every $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$,there exist unique elements $a_0, a_1, \ldots$of $\mathbb{Q}_p$, such that*

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n} \tag{5}$$

For this interpolation series $\sum_{n=0}^{\infty} a_n \binom{x}{n}$,it converges uniformly on $\mathbb{Z}_p$ if and only if $\overset{p}{\lim\limits_{i\rightarrow\infty}} a_i = 0$, $\overset{p}{\lim\limits_{i\rightarrow\infty}}$ means limit under p-adic absolute value.

Definition 2 *.[1] in the ring $\mathbb{Z}_p[[x]]$ of all formal power series in one variable x over the ring $\mathbb{Z}_p$, consider a set $\mathcal{C}(x)$ of all series*

$$s(x) = \sum_{i=0}^{\infty} c_i x^i \ (c_i \in \mathbb{Z}_p, i = 0, 1, 2 \ldots) \tag{6}$$

and $\overset{p}{\lim\limits_{i\rightarrow\infty}} c_i = 0$. Polynomial function is obviously belongs to $\mathcal{C}(x)$.

As $\mathcal{C}(x)$-class functions converge uniformly on $\mathbb{Z}_p$, they are maps $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$.

Now consider Mahler expansions for functions defined by series from $\mathcal{C}(x)$: Let

$$s(x) = \sum_{i=0}^{\infty} s_i \binom{x}{i} \tag{7}$$

using the second kind Stirling number $S_2(k,i)$ ($x^k = \sum_{i=0}^{k} S_2(k,i)x^{\underline{i}}$) and the definition of $\mathcal{C}(x)$, we can deduce that all $\frac{s_i}{i!}$ are p-adic integers.

We have some relations between properties of bijective and measure preserving; transitive and ergodic for the functions over $\mathbb{Z}_p$, that is

Proposition 2 *.[1] A compatible function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is bijective modulo p^k for all $k = 1, 2, ...$ if and only if f preserves measure.*

Proposition 3 *.[1] A compatible function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is ergodic if and only if f is transitive modulo p^k for all $k = 1, 2, ...$(i.e. f is transitive over all finite ring $\mathbb{Z}/p^k\mathbb{Z}$ $k = 1, 2, ...$).*

3 Some properties of Stirling number

Denote $x^{\underline{i}} = x(x-1)(x-2)\cdots(x-i+1)$.

Definition 3 *The first kind Stirling number $S_1(n,k)$, and the second kind Stirling number $S_2(n,k)$ are defined by*

$$x^{\underline{n}} = \sum_{k=0}^{n} S_1(n,k)x^k \tag{8}$$

$$x^n = \sum_{k=0}^{n} S_2(n,k)x^{\underline{k}} \tag{9}$$

There are recursion formulas of these two kind of Stirling numbers

Proposition 4 *[4] (concrete Mathematics)*

$$\begin{aligned} S_1(n,k) &= S_1(n-1,k-1) - (n-1)S_1(n-1,k), 1 \leq k \leq n-1 & (10)\\ S_2(n,k) &= S_1(n-1,k-1) + kS_2(n-1,k), 1 \leq k \leq n-1 & (11)\\ S_2(n,k) &= \sum_{j=k-1}^{n-1} \binom{n-1}{j} S_2(j,k-1) & (12) \end{aligned}$$

From the definition of the two kinds Stirling number, we easily know that $S_1(0,0) = S_2(0,0) = 1, S_1(1,0) = S_2(1,0) = 0, S_1(1,1) = S_2(1,1) = 1$,and when $k < 0$, or $k > n$, $S_1(n,k) = S_2(n,k) = 0$. So further from identities (10),(11), we know that $S_1(n,0) = -(n-1)S_1(n-1,0) = \cdots = (-1)^{n-1}(n-1)!S_1(1,0) = 0$, same calculation shows that $S_2(n,0) = 0.S_1(n,1) = -(n-1)S_1(n-1,1) = \cdots = (-1)^{n-1}(n-1)!S_1(1,1) = (-1)^{n-1}(n-1)!, S_2(n,1) = S_2(n-1,1) = \cdots S_2(1,1) = 1.S_1(n,n) = S_2(n,n) = 1$.We first give some calculation about $S_1(n,k)$ and $S_2(n,k)$, which we will need later.

Lemma 1 *$S_1(n,k) \equiv \binom{\lfloor \frac{n}{2} \rfloor}{k-\lceil \frac{n}{2} \rceil} \bmod 2$, so when $k < \lceil \frac{n}{2} \rceil$, $S_1(n,k)$ is even.*

Proof. From (8), we know that

$$\begin{aligned} \sum_{k=0}^{n} S_1(n,k)x^k &= x(x-1)\cdots(x-n+1) \\ &\equiv x(x+1)x(x+1)\cdots \\ &\equiv x^{\lceil \frac{n}{2} \rceil}(x+1)^{\lfloor \frac{n}{2} \rfloor} \\ &\equiv x^{\lceil \frac{n}{2} \rceil} \sum_{r=0}^{\lfloor \frac{n}{2} \rfloor} x^r \bmod 2 \end{aligned}$$

compare the coefficient of x^k of the two sides, we get the result. ■

Lemma 2 *$S_2(n,2) = 2^{n-1} - 1$; $S_2(n,3) = \frac{3^{n-1}+1}{2} - 2^{n-1}$.*

Proof. From (12) and $S_2(n,1) = 1(n \geq 1)$

$$S_2(n,2) = \sum_{j=1}^{n-1} \binom{n-1}{j} S_2(j,1) = \sum_{j=1}^{n-1} \binom{n-1}{j} = 2^{n-1} - 1 \qquad (13)$$

$$\begin{aligned} S_2(n,3) &= \sum_{j=2}^{n-1} \binom{n-1}{j} S_2(j,2) = \sum_{j=2}^{n-1} \binom{n-1}{j} (2^{j-1} - 1) \qquad (14) \\ &= \frac{1}{2} \sum_{j=2}^{n-1} \binom{n-1}{j} 2^{j-1} - \sum_{j=2}^{n-1} \binom{n-1}{j} \\ &= \frac{1}{2}[3^{n-1} - 1 - 2(n-1)] - [2^{n-1} - 1 - (n-1)] \\ &= \frac{3^{n-1}+1}{2} - 2^{n-1} \end{aligned}$$

■

4 Sufficient and Necessary Condition of single cycle T-Function

In [1], Anashin used his general ergodic result on functions with mahler expansion gived a sufficient and necessary Condition that a $\mathcal{C}(x)$-class function f is single cycle T-function, From formula (7), $f(x)$ can be represented as $f(x) = \sum_{i=0}^{\infty} e_i x^{\underline{i}}$, the condition is

Proposition 5 *The $\mathcal{C}(x)$-class function f is ergodic on $\mathbb{Z}_2$ if and only if*

$$e_0 \equiv 1(\bmod 2), e_1 \equiv 1(\bmod 4), e_2 \equiv 0(\bmod 2), e_3 \equiv 0(\bmod 4), \qquad (15)$$

Here, we firstly use some combinatorial result of stirling numbers to give a proof of the necessary and sufficient condition of functions belong to $\mathcal{C}(x)$ with power series representation, and then, deduce the special result that jin-Song Wang and Wen-Feng Qi got. As our condition is more simple than theirs, we can further get a Counting formula for polynomial type single cycle T-function.

Theorem 2 *Let the $\mathcal{C}$-function f be represented via power series:$f(x) = \sum_{i=0}^{\infty} c_i x^i$, $c_i \in \mathbb{Z}_2$, $i = 0, 1, 2, \ldots$. Then the function f is ergodic on $\mathbb{Z}_2$ if and only if the following congruences hold simultaneously:*

$$\begin{aligned} c_3 + c_5 + c_7 + \cdots &\equiv 2c_2 (\bmod 4) \quad (16)\\ c_4 + c_6 + c_8 + \cdots &\equiv c_1 + c_2 - 1 (\bmod 4) \quad (17)\\ c_1 &\equiv 1 (\bmod 2) \quad (18)\\ c_0 &\equiv 1 (\bmod 2) \quad (19)\end{aligned}$$

Proof. From above proposition, we just need to prove that this condition is equivalent to (15).

firstly, we prove that if there is (15), then we have (16) and so on. At first, we surely have

$$\begin{aligned} c_0 &= e_0 \equiv 1 (\bmod 2)\\ c_1 &\equiv e_1 + e_2 \equiv 1 (\bmod 2)\end{aligned}$$

so, we have identities (18) (19). As

$$\begin{aligned} f(x) &= \sum_{j=0}^{\infty} c_j x^j = \sum_{j=0}^{\infty} c_j (\sum_{i=0}^{j} S_2(j,i) x^{\underline{i}}) \quad (20)\\ &= \sum_{i=0}^{\infty} (\sum_{j=i}^{\infty} S_2(j,i) c_j) x^{\underline{i}}\end{aligned}$$

So, we have

$$e_1 = \sum_{j=1}^{\infty} S_2(j,1) c_j \overset{S_2(j,1)=1(j\geq 1)}{\equiv} \sum_{j=1}^{\infty} c_j \quad (21)$$

$$e_2 = \sum_{j=2}^{\infty} S_2(j,1) c_j \overset{S_2(j,2)=2^{j-1}-1(j\geq 1)}{=} \sum_{j=2}^{\infty} (2^{j-1} - 1) c_j \quad (22)$$

so from (21), we know

$$\sum_{j=1}^{\infty} c_j \equiv e_1 \equiv 1(\mathrm{mod}\, 4) \tag{23}$$

$$\sum_{j=2}^{\infty} c_j \equiv e_2 \equiv 0(\mathrm{mod}\, 2)$$

$$c_2 + (\sum_{j=3}^{\infty} c_j) \equiv e_2(\mathrm{mod}\, 4)$$

$$c_1 \equiv \sum_{j=1}^{\infty} c_j - \sum_{j=2}^{\infty} c_j \equiv 1(\mathrm{mod}\, 2) \tag{24}$$

$$\begin{aligned} e_3 &= \sum_{j=3}^{\infty} S_2(j,3)c_j \overset{S_2(j,3)=\frac{3^{j-1}+1}{2}-2^{j-1}}{=} \sum_{j=3}^{\infty}(\frac{3^{j-1}+1}{2} - 2^{j-1})c_j \\ &\equiv \sum_{j=3}^{\infty}(1+(j-1)+\frac{(j-1)(j-2)}{2}\cdot 2)c_j \\ &\equiv \sum_{j=3}^{\infty}(1+(j-1)+(j-1)(j-2))c_j(\mathrm{mod}\, 4) \end{aligned}$$

so, we have

$$e_3 \equiv \sum_{j=3, j \text{ even}}^{\infty} 2c_j + \sum_{j=3, j \text{ odd}}^{\infty} c_j \equiv 0(\mathrm{mod}\, 4) \tag{25}$$

from (23),(24), we have

$$(c_2+c_4+c_6+\cdots)+(c_3+c_5+c_7+\cdots)+2c_{1,1} \equiv 0(\mathrm{mod}\, 4) \tag{26}$$

(25)−(23),

$$\begin{aligned} c_4+c_6+c_8+\cdots &\equiv c_2+2c_{1,1} \\ &\equiv c_1+c_2-1(\mathrm{mod}\, 4) \end{aligned} \tag{27}$$

(26)−(27),

$$c_2+c_3+c_5+c_7+\cdots+2c_{1,1} \equiv -c_1-c_2+1(\mathrm{mod}\, 4)$$

⇒

$$c_3+c_5+c_7+\cdots \equiv 2c_2(\mathrm{mod}\, 4)$$

so, we proved (16),(17). Then we prove the inverse direction. we have $e_0 \equiv c_0 \equiv c_1 \equiv 1(\mathrm{mod}\, 2), c_3+c_5+c_7+\cdots \equiv 2c_2(\mathrm{mod}\, 4), c_4+c_6+c_8+\cdots \equiv$

$c_1+c_2-1(\bmod 4)$.From (16),(17) and (21), we have

$$\begin{aligned} e_1 &\equiv \sum_{j=1}^{\infty} c_j \equiv c_1+c_2+2c_2+c_1+c_2-1 \\ &\equiv 2c_1-1 \equiv 1(\bmod 4) \end{aligned}$$

$$e_2 \equiv \sum_{j=2}^{\infty} c_j \equiv c_1+c_2+c_3+\cdots-c_1 \equiv 1-1 \equiv 0(\bmod 2)$$

$$\begin{aligned} e_3 &\equiv \sum_{j=3,j \text{ even}}^{\infty} 2c_j + \sum_{j=3,j \text{ odd}}^{\infty} c_j \overset{(16),(17)}{\equiv} 2c_2+2(c_1+c_2-1) \\ &\equiv 2c_1-2 \equiv 0(\bmod 4) \end{aligned}$$

so we prove the theorem. ■

Then we show that Jin-Song Wang and Wen-Feng Qi's result on the sufficient and necessary condition of single cycle polynomial T-function is our special case. As we said that, polynomial T-function surely belongs to $\mathcal{C}$-class function. Their result is $f(x)=c_0+c_1x+c_2x^2+\cdots+c_mx^m$ with integer coefficients modulo $2^n(n\geq 3)$ is a single cycle T-function, if and only if c_0, c_1 are odd, $\triangle_1,\triangle_2$ are even, $\triangle_1+\triangle_2+2c_{1,0}\equiv 0 \bmod 4$, and $\triangle_1+2c_{2,0}+2c_{1,1}\equiv 0 \bmod 4$, where $\triangle_1=(c_2+c_4+\cdots),\triangle_2=(c_3+c_5+\cdots)$. From (16),(17),(18),(19), we easily get c_0, c_1 are odd, $\triangle_1,\triangle_2$ are even.

Corollary 1 *For polynomial single cycle T-function, theorem 2 is equivalent to c_0, c_1 are odd, $\triangle_1,\triangle_2$ are even, $\triangle_1+\triangle_2+2c_{1,0}\equiv 0 \bmod 4$, and $\triangle_1+2c_{2,0}+2c_{1,1}\equiv 0 \bmod 4$.*

Proof. "⇒" as $c_0\equiv c_1\equiv 1(\bmod 2)$, and (16),(17), we have

$$\begin{aligned} c_2+(c_4+c_6+c_8+\cdots)+(c_3+c_5+c_7+\cdots) &\equiv c_2+c_1+c_2-1+2c_2 \\ &\equiv 2c_{1,1}(\bmod 4) \end{aligned}$$

so we get $\triangle_1+\triangle_2+2c_{1,1}\equiv 0 \bmod 4$

$$\begin{aligned} c_2+(c_4+c_6+c_8+\cdots) &\equiv c_2+c_1+c_2-1 \\ &\equiv 2c_{2,0}+2c_{1,1} \bmod 4 \end{aligned}$$

so we get $\triangle_1+2c_{2,0}+2c_{1,1}\equiv 0 \bmod 4$.

"⇐" we have $c_0\equiv c_1\equiv 1(\bmod 2)$,

$$\triangle_1+\triangle_2+2c_{1,0} \equiv 0 \bmod 4 \quad (28)$$

$$\triangle_1+2c_{2,0}+2c_{1,1} \equiv 0 \bmod 4 \quad (29)$$

(28)−(29), ⇒ $\triangle_2-2c_{2,0}\equiv 0(\bmod 4)$, i.e

$$c_3+c_5+c_7+\cdots\equiv 2c_2(\bmod 4)$$

from (29), we have $c_2 + c_4 + c_6 + \cdots + 2c_{2,0} + 2c_{1,1} \equiv 0 \bmod 4 \Rightarrow$

$$\begin{aligned} c_4 + c_6 + c_8 + \cdots &\equiv 3c_2 + 2c_{2,0} + 2c_{1,1} \\ &\equiv c_2 + 2c_{1,1} \\ &\equiv c_2 + c_1 - 1 (\bmod 4) \end{aligned}$$

■

5 Formula for the number of ergodic polynomial functions over $\mathbb{Z}/2^n\mathbb{Z}$ and degree level structure

In [5], Wenying Zhang and Chuan-Kun Wu give the number of single-cycle T-functions over $\mathbb{Z}/2^n\mathbb{Z}$, that is 2^{2^n-n-1}. Here, we can even known the number of single-cycle polynomial type T-functions over $\mathbb{Z}/2^n\mathbb{Z}$ using more simple condition (15). Firstly, using two kinds Stirling numbers, we can give one to one transformation between the representation of polynomial and falling factorial series.

$$\begin{aligned} f(x) &= \sum_{i=0}^{m} e_i x^{\underline{i}} = \sum_{i=0}^{m} e_i (\sum_{j=0}^{i} S_1(i,j) x^j) = \sum_{j=0}^{m} (\sum_{i=j}^{m} S_1(i,j) e_i) x^j && (30) \\ f(x) &= \sum_{j=0}^{m} c_j x^j = \sum_{j=0}^{m} c_j (\sum_{i=0}^{j} S_2(j,i) x^{\underline{i}}) = \sum_{i=0}^{m} (\sum_{j=i}^{m} S_2(j,i) c_j) x^{\underline{i}} && (31) \end{aligned}$$

The result is

Theorem 3 *Denot $N_{m,n}$ is the number of polynomial type T-functions defined on $\mathbb{Z}/2^n\mathbb{Z}$, whose degree are not exceed m, and transitive(single-cycle) on all $\mathbb{Z}/2^k\mathbb{Z}, k \geq 2$, $N_{m,n}$ is*

$$N_{m,n} = \left\{ \begin{array}{ccc} 0, & & m = 0 \\ 1, & n = 1 & m = 1 \\ 2^{2n-3}, & \textit{for fixed } n \geq 2 & m = 1 \\ 2^{3n-4}, & \textit{for fixed } n \geq 2 & m = 2 \\ 2^{mn+n-6}, & \textit{for fixed } n \geq 2 & \textit{for fixed } m \geq 3 \end{array} \right. \qquad (32)$$

Proof. If we have a polynomial $f(x) = \sum_{i=0}^{n} e_i x^{\underline{i}}$, when $m = 0$, there is no single-cycle polynomial T-functions.

1. When $m = 1$, $n = 1$, there is only one single-cycle polynomial, i.e $f(x) = x + 1$.

2. When $m = 1$, $n = 1$, we know that there are only 1-degree polynomials over $\mathbb{Z}/2\mathbb{Z}$; when $n \geq 2$, from $e_0 \equiv 1(\bmod 2), e_1 \equiv 1(\bmod 4), e_0$ has 2^{n-1} choices, e_1 has 2^{n-2} choices, so there are 2^{2n-3} single-cycle 1-degree polynomial T-functions.

3. When $m = 2$, we naturally demand $n \geq 2$, from $e_0 \equiv 1(\bmod 2), e_1 \equiv 1(\bmod 4), e_2 \equiv 0(\bmod 2), e_0$ has 2^{n-1} choices, e_1 has 2^{n-2} choices, e_2 has 2^{n-1} choices,so there are 2^{3n-4} single-cycle 2-degree polynomial T-functions.

4. When $m = 3$, from $e_0 \equiv 1(\bmod 2), e_1 \equiv 1(\bmod 4), e_2 \equiv 0(\bmod 2), e_3 \equiv 0(\bmod 4), e_0$ has 2^{n-1} choices, e_1 has 2^{n-2} choices, e_2 has 2^{n-1} choices, e_3 has 2^{n-2} choices, so there are 2^{4n-6} single-cycle 3-degree polynomial T-functions. When $m > 3$,the later coefficients $e_{i,i>3}$ have no restriction, so there are

$$2^{(n-1)+(n-2)+(n-1)+(n-2)+n(m+1-4)} = 2^{mn+n-6} \tag{33}$$

single-cycle m-degree polynomial T-functions.

So, we have the table above(32). ■

Remark 1 *a. In (32), we look the different polynomials but raise the same transformation on $\mathbb{Z}/2^n\mathbb{Z}$ as different ones. In [6], M.V.Larin give the number of single-cycle polynomial transformation over $\mathbb{Z}/2^n\mathbb{Z}, n \geq 3$.But at there, he look the different polynomials that raise the same transformation on $\mathbb{Z}/2^n\mathbb{Z}$ as a single one. For example, in [6], he give a table of all transitive polynomials over $\mathbb{Z}/8\mathbb{Z}$ in his sense*

$$\begin{array}{llll}
x+1 & 5x+1 & 2x^2+3x+1 & 2x^2+7x+1 \\
x+3 & 5x+3 & 2x^2+3x+3 & 2x^2+7x+3 \\
x+5 & 5x+5 & 2x^2+3x+5 & 2x^2+7x+5 \\
x+7 & 5x+7 & 2x^2+3x+7 & 2x^2+7x+7
\end{array}$$

but, we still have $1+x+4x^2(0 \to 1 \to 6 \to 7 \to 4 \to 5 \to 2 \to 3 \to 0)$,raise the same orbit with $5x+1$; $1+7x+6x^2(0 \to 1 \to 6 \to 3 \to 4 \to 5 \to 2 \to 7 \to 0)$,raise the same orbit with $2x^2+3x+1$,and so on. So in our sense, we have a table of all transitive $2-$degree polynomials over $\mathbb{Z}/8\mathbb{Z}$ as

$$\begin{array}{llllll}
x+1 & 5x+1 & 2x^2+3x+1 & 2x^2+7x+1 & 4x^2+x+1 & 6x^2+3x+1 \\
x+3 & 5x+3 & 2x^2+3x+3 & 2x^2+7x+3 & 4x^2+x+3 & 6x^2+3x+3 \\
x+5 & 5x+5 & 2x^2+3x+5 & 2x^2+7x+5 & 4x^2+x+5 & 6x^2+3x+5 \\
x+7 & 5x+7 & 2x^2+3x+7 & 2x^2+7x+7 & 4x^2+x+7 & 6x^2+3x+7
\end{array}$$

$$\begin{array}{ll}
4x^2+5x+1 & 6x^2+7x+1 \\
4x^2+5x+3 & 6x^2+7x+3 \\
4x^2+5x+5 & 6x^2+7x+5 \\
4x^2+5x+7 & 6x^2+7x+7
\end{array}$$

b. When$1 \leq n < 3$, a single cycle orbit on $\mathbb{Z}/2^n\mathbb{Z}$ which can be represented by polynomial and transitive over all $\mathbb{Z}/2^k\mathbb{Z}(k \geq n)$, is also a polynomial transformation and transitive on $\mathbb{Z}/2^k\mathbb{Z}(0<k < n)$. When $n \geq 3$, polynomial single cycle orbit on $\mathbb{Z}/2^n\mathbb{Z}$, which can be transitive over all $\mathbb{Z}/2^k\mathbb{Z}(k \in \mathbb{N})$.Because, if a polynomial transitive on $\mathbb{Z}/2^3\mathbb{Z}$, it will transitive on all $\mathbb{Z}/2^k\mathbb{Z}(k \in \mathbb{N})$.

$\mathcal{C}$-function can be represented as (7), and we have

Proposition 6 *[1] A function $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ with mahler expansion is $0(\mathrm{mod}\, p^k)$ for all $v \in \mathbb{Z}_p$ if and only if for all coefficients of its Mahler expansion (7) are 0 modulo p^k,i.e.*

$$|s_i|_p \leq p^k, for\ all\ i \in \mathbb{N}_0$$

In our case, when $\mathcal{C}$-function $f(x) = \sum_{i=0}^{m} e_i x^{\underline{i}}, ord_2(j!e_j) \geq n$, we have $\sum_{i=j}^{m} e_j v^{\underline{j}} \equiv 0(\mathrm{mod}\, 2^n)$ for all $v \in \mathbb{Z}_p$. So, to a single-cycle polynomial, fixed n, when degree $m \geq j$, it must raise a transformation coincides with a transformation on $\mathbb{Z}/2^n\mathbb{Z}$ induced by a smaller degree polynomial.

Proposition 7 *[6] (M.V.Larin. Transitive polynomial transformations of residue class rings) The number of transitive polynomial transformations of residue class ring $\mathbb{Z}/2^n\mathbb{Z}$ is For $p \notin \{2,3\}, n = 1$,there are $(p-1)!$Transitive polynomial transformations; for $n = 2$, the number is $(p-2)!(p-1)^{p+1}p^{p-1}$; $n \geq 3$,it is $(p-2)!(p-1)^{p+1}p^{p-1+\varepsilon(p,3)+\cdots+\varepsilon(p,n)}$, where $\varepsilon(p,k) = min(i \geq 0 : ord_p(i!) \geq k)$.For $p = 2, n = 3$,there are 16 Transitive polynomial transformations, $n \geq 4$, the number is $2^{4+\varepsilon(2,4)+\cdots+\varepsilon(2,n)}$;For $p = 3, n = 3$,there are $2^5 3^{10}$ Transitive polynomial transformations, $n \geq 4$, the number is $2^5 3^{10+\varepsilon(3,4)+\cdots+\varepsilon(3,n)}$.*

So, from above propositions and proposition (5), we can deduce the smallest degree m, that the transitive polynomials of degree not exceed m constitute the whole set of single-cycle polynomial transformations over $\mathbb{Z}/2^n\mathbb{Z}$. Actually, now, we can know how many single-cycle T-functions over $\mathbb{Z}/2^n\mathbb{Z}$ are not polynomial type.

Theorem 4 *For fixed $n \in \mathbb{N}$,when $n = 1, 2, 3$, all single-cycles that induced by T-function can be represented by polynomial; when $n \geq 4$, there are $2^{2^n-n-1} - 2^{4+\varepsilon(2,4)+\cdots+\varepsilon(2,n)}$single-cycles in all T-function induced single-cycles on $\mathbb{Z}/2^n\mathbb{Z}$ that not induced by polynomial.*

Proof. On $\mathbb{Z}/2^n\mathbb{Z}$, the single-cycle T-function can be represented as

$$f(\sum_{i=0}^{n-1} \chi_i 2^i) = \sum_{i=0}^{n-1} \Psi_i(\chi_0, \ldots, \chi_i) 2^i,$$

where $\Psi_i(\chi_0, \ldots, \chi_i) = \chi_i \oplus \varphi_i(\chi_0, \ldots, \chi_{i-1}), \varphi_0 = 1$,

$$\varphi_i(\chi_0, \ldots, \chi_{i-1}) = \chi_0 \chi_1 \cdots \chi_{i-1} \oplus \eta(\chi_0, \ldots, \chi_{i-1}),$$

where $\eta(\chi_0, \ldots, \chi_{i-1}), i = 1, 2, \ldots n-1$ are Boolean functions of i variables with algebraic degree being less than i, and there are 2^{2^i-1} such Boolean functions, so there are $2^{(2-1)+(2^2-1)+(2^3-1)+\cdots+(2^{n-1}-1)} = 2^{2^n-n-1}$single-cycle T-functions on $\mathbb{Z}/2^n\mathbb{Z}$, and they raise different permutations, i.e. different single-cycle orbits on $\mathbb{Z}/2^n\mathbb{Z}$. We already know that, there is only one polynomial single-cycle $f(x) = x+1$, and two polynomial single-cycles $f(x) = x+1; f(x) = x+3$ when $n = 1$ and $n = 2$.And from proposition [7], there are 16 polynomial single-cycles when $n = 3$.But $2^{2^n-n-1} = 1, 2, 16$ when $n = 1, 2, 3$.So, all single-cycles that induced by T-function can be represented by polynomial. Proposition [7] shows that there are $2^{4+\varepsilon(2,4)+\cdots+\varepsilon(2,n)}$ single-cycle polynomial transformations on $\mathbb{Z}/2^n\mathbb{Z}$, so we have $2^{2^n-n-1} - 2^{4+\varepsilon(2,4)+\cdots+\varepsilon(2,n)}$ non-polynomial single-cycles in all T-function induced single cycles. ■

We have a table as follow

Ring:$\mathbb{Z}/2^n\mathbb{Z}$	$n=1$	$n=2$	$n=3$	for fixed $n \geq 4$
number of T-function single-cycles	1	2	16	2^{2^n-n-1}
number of polynomial single-cycles	1	2	16	$2^{4+\varepsilon(2,4)+\cdots+\varepsilon(2,n)}$
rate of polynomial T-function single-cycles in all T-function single-cycles	1	1	1	$2^{n+5+[\varepsilon(2,4)+\cdots+\varepsilon(2,n)-2^n}$

Simple calculation shows that $\varepsilon(2,4) = 6, \varepsilon(2,5) = 8, \varepsilon(2,6) = 8, \varepsilon(2,7) = 8, \varepsilon(2,8) = 10, \ldots$.Because there is a exponential function about n, rate will decrease very quickly, for example, the first 10 values are$1, 1, 1, 0.5, 0.0039, 0.466 \times 10^{-9}, 0.129 \times 10^{-25}, 0.778 \times 10^{-61}, 0.550 \times 10^{-134}, 0.336 \times 10^{-284}$.

Now, for fixed n, we can know, what's the least degree m that all the single-cycle polynomial transformations can be expressed as the polynomials that degree does not exceed m over $\mathbb{Z}/2^n\mathbb{Z}$.

Theorem 5 *When $n = 1$,the only one single-cycle polynomial transformations is $x + 1$; $n = 2$,the whole single-cycle polynomial transformations are $x + 1, x + 3$; $n = 3$,the whole 16 single-cycle polynomial transformations can be represented by single-cycle polynomials degree not exceed 2;when fixed $n \geq 4$,denote*

$$T(m) = \sum_{i=4}^{m} ord_2(i!), \quad S(n) = \sum_{j=4}^{n} \varepsilon(2,j), \varepsilon(2,k) = min(i \geq 0 : ord_2(i!) \geq k)$$

the least degree m is the integer that satisfy the following equation

$$n(m+1) - 8 - T(m) = 4 + S(n) \tag{34}$$

Proof. When $n = 1, 2, 3$,the result is simple followed by the above theorem. Fixed $n \geq 4$, if we have two polynomials

$$f(x) = \sum_{i=0}^{m} e_i x^{\underline{i}}, \tilde{f}(x) = \sum_{i=0}^{m} \tilde{e}_i x^{\underline{i}}$$

that raise the same single transformation on $\mathbb{Z}/2^n\mathbb{Z}$, then

$$f(\upsilon) - \tilde{f}(\upsilon) = \sum_{i=0}^{m} e_i \upsilon^{\underline{i}} - \sum_{i=0}^{m} \tilde{e}_i \upsilon^{\underline{i}} = \sum_{i=0}^{m} (e_i - \tilde{e}_i) \upsilon^{\underline{i}} \equiv 0 (\mathrm{mod}\, 2^n), \text{for all } \upsilon \in \mathbb{Z}_p \tag{35}$$

we always assume $deg(f(v) \geq deg(\tilde{f}(v))$, $e_{i,i>deg(f(v)} = 0 = e_{j,j>deg(\tilde{f}(v))}$. From proposition[6], we have

$$\begin{cases} ord_2(e_0 - \tilde{e}_0) \geq n & i = 0 \\ ord_2(e_1 - \tilde{e}_1) \geq n & i = 1 \\ 1 + ord_2(e_2 - \tilde{e}_2) \geq n & i = 2 \\ 1 + ord_2(e_3 - \tilde{e}_3) \geq n & i = 3 \\ ord_2(i!) + ord_2(e_i - \tilde{e}_i) \geq n & i \geq 4 \end{cases} \tag{36}$$

$ord_2(e_0 - \tilde{e}_0) \geq n$ demands $e_0 = \tilde{e}_0$ On $\mathbb{Z}/2^n\mathbb{Z}$, by the same reason, $e_1 = \tilde{e}_1$ On $\mathbb{Z}/2^n\mathbb{Z}$. For fixed e_2, $\tilde{e}_{2,n-1}$ can be different from $e_{2,n-1}$,so there are two choices for $\tilde{e}_{2,n-1}$,i.e. $\tilde{e}_{2,n-1} = e_{2,n-1}$ or $\tilde{e}_{2,n-1} \neq e_{2,n-1}$,so there are two choices for $\tilde{e}_2$.The same reason shows that, $\tilde{e}_3$ have two choices on $\mathbb{Z}/2^n\mathbb{Z}$. By $ord_2(i!) + ord_2(e_i - \tilde{e}_i) \geq n, i \geq 4$,we know that the first $(n - ord_2(i!))$-digits must be equal, so $\tilde{e}_i$ has $2^{ord_2(i!)}$ choices. So for fixed $m \geq 3$,there are $2^{1+1+\sum_{i=4}^{m} ord_2(i!)} = 2^{2+T(m)}$ polynomials raise the same single cycle transformation with $f(x)$. Actually from (33), there are

$$2^{mn+n-6}/2^{2+T(m)} = 2^{m(n+1)-8-T(m)} \tag{37}$$

different single-cycle polynomial transformations. Combine with proposition [7]

$$2^{m(n+1)-8-T(m)} = 2^{4+\varepsilon(2,4)+\cdots+\varepsilon(2,n)}$$

$\Rightarrow$

$$m(n+1) - 8 - T(m) = 4 + \varepsilon(2,4) + \cdots + \varepsilon(2,n) = 4 + S(n)$$

solve this equation about m,we get the least degree. ■

Remark 2 *a. In fact, we get another formula of transitive polynomial transformation on residue class rings $\mathbb{Z}/2^n\mathbb{Z}$ different from M.V.Larin[6]. Our equation (37) has another parameter m, which can tell us more information about degree. For fixed n, $T(m)$ is a function corresponding with $m!$, $m(n+1) - 8$ is a linear function of m,so, while m increase, $m(n+1) - 8 - T(m)$ will be negative, this m is surely meaningless.*

b. Actually, from $ord_2(i!) + ord_2(e_i - \tilde{e}_i) \geq n, (i \geq 3)$, and $n \geq ord_2(e_i - \tilde{e}_i) \geq 0$, we surely have $m \leq \min\{j, ord_2(j!) \geq n\}$.

Acoording to above theorem, we can do some calculation. For example, we can get the following table

$\mathbb{Z}/2^n\mathbb{Z}$	$2^{4+S(n)} = 2^{m(n+1)-8-T(m)}$	m
$n = 4$	2^{10}	5
$n = 5$	2^{18}	7
$n = 6$	2^{26}	7
$n = 7$	2^{34}	7
$n = 8$	2^{44}	9
$n = 9$	2^{56}	11
$\vdots$	$\vdots$	$\vdots$

6 Linear Equation on ergodic power-series T-Function

in the work [7] (Linear Properties in T-Functions) Molland.H and Tor Helleseth give a linear equation of sequence generated by $x_i = x_{i-1}^2 \vee C + x_{i-1} \bmod 2^n$ proposed by Klimov and Shamir.That is

$$x_{i,j} + x_{i+2^{j-1},j} + x_{i,j-1} + a_2 x_{i,1} + a_1 x_{i,0} + a_0 = 0 \bmod 2$$

where $x_{i,j}$ is the j-th digit of x_i, and a_2, a_1, a_0 are constants defined by the binary digit of C. Jin-Song Wang and Wen-Feng Qi calculate a similar equation for single cycle polynomial T-function, that is, given an initial point $x_0 \in \mathbb{Z}/2^n\mathbb{Z}$, $x_i = f(x_{i-1}), f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$,then, there is a linear equation

$$x_{i+2^{j-1},j} = x_{i,j} + x_{i,j-1} + ajA_{i,2} + a(j-1) + b \bmod 2, 3 \leq j \leq n-1$$

$A_{i,2}$ is a sequence of period 4 and a, b are constants determined by the coefficients c_i.

Now we generalized their result to our general case $\mathcal{C}(x)$-class functions. From the definition of $\mathcal{C}(x)$-class function, integer coefficients polynomial T-function surely belongs to this function class. (to n-degree polynomial T-function, we can identify $c_i = 0, i > n$). There are many other kinds of T-functions besides polynomial T-function in $\mathcal{C}(x)$. for example $f(x) = x + (1 + p^3 x)^{-1}; f(x) = a^x = \sum_{i=0}^{\infty} p^i r^i \binom{x}{i}$, where p is odd, and $a \equiv 1 (\bmod\, p); f(x) = (1+4r)^x, p = 2, r \in \mathbb{Z}_2$.

If $f(x) = c_0 + c_1 x + \cdots + c_m x^m + \cdots$ is a $\mathcal{C}$-class ergodic transformation over $\mathbb{Z}_2$, as the theorem [2] shows, c_0, c_1 are odd, and $\triangle_1 = (c_2 + c_4 + c_6 \cdots), \triangle_2 = (c_3 + c_5 + c_7 \cdots)$ are even. We should mention a result of Anashin about the ergodic transformation over $\mathbb{Z}_2$.

Proposition 8 *A function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is 1-Lipschitz and measure-preserving(re spectively, is 1-Lipschitz and ergodic) if and only if it can be represented in the form $f(x) = c + x + 2 \cdot v(x)$ (respectively, in the form $f(x) = 1 + x + 2 \cdot \triangle v(x), \triangle v(x) = v(x+1) - v(x)$), where $c \in \mathbb{Z}_2$ and $v(x)$ is a 1-Lipschitz function.*

As the identities (16)(17)(18)(19), we also have some similar identities with Jin-Song Wang and Wen-Feng Qi's. That is

$$\begin{aligned}
\sum_{j=2}^{\infty} c_j j &\equiv \sum_{j=2, j \text{ is odd}}^{\infty} c_j j \equiv 0 \bmod 2, && (38)\\
\sum_{j=2}^{\infty} c_j j &\equiv 2(\triangle_2/2 + \sum_{j=2, j\equiv 2,3 \bmod 4}^{\infty} c_{j,0}) \bmod 4 && (39)\\
\sum_{j=2}^{\infty} c_j j(j-1) &\equiv 2 \sum_{j=2, j\equiv 2,3 \bmod 4}^{\infty} c_{j,0} \bmod 4, && (40)\\
c_1^{2^{n-1}} &\equiv 1 \bmod 2^{n+1} && (41)\\
c_1^{2^{n-2}} &\equiv 1 + 2^n(c_{1,1} \oplus c_{1,2}) \bmod 2^{n+1} && (42)\\
c_0(1 + c_1 + \cdots + c_1^{2^{n-1}-1}) &\equiv 2^{n-1}(c_{1,1} \oplus 1) + \\
& \quad 2^n(c_{0,1} \oplus c_{0,1}c_{1,1} \oplus c_{1,1} \oplus c_{1,2}) \bmod 2^{n+1} && (43)
\end{aligned}$$

Sequence $\{x_i\}$, generated by iterated the $\mathcal{C}(x)$-class function f, is

$$x_1 = f(x_0) = c_0 + c_1 x_0 + \sum_{j=2}^{\infty} c_j x_0^j$$

As $\mathcal{C}(x)$-class function converges everywhere on $\mathbb{Z}_p$,so $f(x_0)$ converges to a 2-adic integer x_1.

$$\begin{aligned}
x_2 &= c_0(1 + c_1) + c_1^2 x_0 + \sum_{j=2}^{\infty} c_j x_1^j + c_1 \sum_{j=2}^{\infty} c_j x_0^j \\
&\vdots \\
x_{2^{n-1}} &= c_0(1 + c_1 + \cdots + c_1^{2^{n-1}-1}) + c_1^{2^{n-1}} x_0 + \\
& \quad \sum_{i=0}^{2^{n-1}-1-i} c_1^{2^{n-1}-1-i} \sum_{j=2}^{\infty} c_j x_i^j && (44)
\end{aligned}$$

use above identities, we can get

$$\begin{aligned}
x_{2^{n-1}} &\equiv 2^{n-1}(c_{1,1} \oplus 1) + 2^n(c_{0,1} \oplus c_{0,1}c_{1,1} \oplus c_{1,1} \oplus c_{1,2}) && (45)\\
& \quad + x_0 + \sum_{j=2}^{\infty} c_j (\sum_{i=0}^{2^{n-1}-1} c_1^{2^{n-1}-1-i} x_i^j) \bmod 2^{n+1}
\end{aligned}$$

and

$$\begin{aligned}
& \sum_{j=2}^{\infty} c_j \big(\sum_{i=0}^{2^{n-1}-1} c_1^{2^{n-1}-1-i} x_i^j \big) \bmod 2^{n+1} \\
\equiv \; & \sum_{j=2}^{\infty} c_j \{ \sum_{i=0}^{2^{n-1}-1} c_1^{2^{n-1}-1-i} [(x_i \bmod 2^{n-1})^j + j x_{i,n-1} 2^{n-1} (x_i \bmod 2^{n-1})^{j-1} \\
& + j x_{i,n} 2^n (x_i \bmod 2^{n-1})^{j-1}] \} \bmod 2^{n+1}
\end{aligned}$$

Almost the same caculation with Jin-Song Wang and Wen-Feng Qi

$$\begin{aligned}
& \sum_{j=2}^{\infty} c_j j x_{i,n} 2^n (x_i \bmod 2^{n-1})^{j-1} \\
\equiv \; & 2^n \{ \sum_{j=2}^{\infty} c_j j \sum_{i=0}^{2^{n-1}-1} c_{1,0} (x_{i,n} x_{i,0}) \bmod 2 \} = 0 \bmod 2^{n+1} \\
\equiv \; & 0
\end{aligned} \tag{46}$$

$$\begin{aligned}
& 2^{n-1} \{ \sum_{j=2}^{\infty} c_j j \big(\sum_{i=0}^{2^{n-1}-1} c_1^{2^{n-1}-1-i} x_{i,n-1} (x_i \bmod 2^{n-1})^{j-1} \big) \bmod 4 \} \bmod 2^{n+1} \\
\equiv \; & 2^{n-1} \{ \sum_{j=2}^{\infty} c_j j \big(\sum_{i=0}^{2^{n-1}-1} c_1^{2^{n-1}-1-i} (x_{i,n-1} x_{i,0} + 2(j-1) x_{i,0}^{j-2} x_{i,1} x_{i,n-1}) \big) \bmod 4 \} \bmod 2^{n+1} \\
\equiv \; & 2^{n-1} \big(\sum_{j=2}^{\infty} c_j j \big(\sum_{i=0}^{2^{n-1}-1} x_{i,n-1} x_{i,0} \bmod 2 \big) \bmod 4 \big) \bmod 2^{n+1} \\
\equiv \; & 2^n a A_{0,n-1} \bmod 2^{n+1}
\end{aligned} \tag{47}$$

where $a = \triangle_2/2 + \sum_{j=2, j \equiv 2,3 \bmod 4}^{\infty} c_{j,0} \bmod 2$, $A_{0,n-1} = \sum_{i=0}^{2^{n-1}-1} x_{i,n-1} x_{i,0} \bmod 2$.The same caculation with [2], $A_{i,n} = \sum_{k=0}^{2^n-1} x_{i+k,n} x_{i+k,0} \bmod 2 = A_{0,n} \oplus d_i$, $\{d_i\}$ is a sequence of period 4 $(d_0, d_1, d_2, d_3) = (0, x_{0,0}, 1, x_{0,0} \oplus 1)$; Another part denoted by

$$\begin{aligned}
B_n \; = \; & \sum_{j=2}^{\infty} c_j \big(\sum_{i=0}^{2^{n-1}-1} c_1^{2^{n-1}-1-i} (x_i \bmod 2^{n-1})^j \big) \bmod 2^{n+1} (n \geq 4) \\
= \; & 2^{n-1} c_{1,1} + 2^n ([c_{2,0} \triangle_1 /2 \bmod 4]_1 + c_{2,1} + c_{1,1} c_{2,0} \\
& + \sum_{j=6, j \equiv 2 \bmod 4}^{m} c_j + a \sum_{l=2}^{n-2} A_{0,l} + c_{1,1} x_{0,0}) \bmod 2^{n+1}
\end{aligned} \tag{48}$$

denot

$$\begin{aligned} b &= c_{0,1} + c_{0,1}c_{1,1} + c_{1,1} + c_{1,2} + c_{2,1} + c_{1,1}c_{2,0} \\ & +[c_{2.0} + \triangle_1/2 \bmod 4]_1 + \sum_{j=6, j\equiv 2 \bmod 4}^{\infty} c_{j,0} \bmod 2 \end{aligned}$$

Combine above identities. we get

$$x_{2^{n-1},n} = x_{0,n} + x_{0,n-1} + c_{1,1}x_{i,0} + a\sum_{l=2}^{n-1} A_{0,l} + b \bmod 2, (n \geq 5) \tag{49}$$

As the above equation is correct for all x_0, it is also correct for the sequence shift i positions, that is,

$$x_{i+2^{n-1},n} = x_{i,n} + x_{i,n-1} + c_{1,1}x_{i,0} + a\sum_{l=2}^{n-1} A_{i,l} + b \bmod 2, (n \geq 5) \tag{50}$$

As $x_i \bmod 2^n$ contains all the subsequences $x_i \bmod 2^j (1 \leq j \leq n-1)$, then the above equation is correct for all $j (4 \leq j \leq n-1)$, that is

$$x_{i+2^{j-1},j} = x_{i,j} + x_{i,j-1} + c_{1,1}x_{i,0} + a\sum_{l=2}^{j-1} A_{i,l} + b \bmod 2 \ (3 \leq j \leq n-1) \tag{51}$$

From [2], we know

$$A_{i,j} = \left\{ \begin{array}{cc} A_{i,j-1}, & j > 4 \\ A_{i,2} + a(j-2), & j = 3 \end{array} \right. \bmod 2$$

then

$$A_{i,j} = A_{i,j-1} = \cdots = A_{i,2} + a(j-2) \bmod 2 \tag{52}$$

then, from (51)(52), we have

$$x_{i+2^{j-1},j} = x_{i,j} + x_{i,j-1} + ajA_{i,2} + a(j-1) + b \bmod 2 (3 \leq j \leq n-1)$$

So, sum up, we get a theorem generalized the result of [2].

Theorem 6 *For an ergodic $\mathcal{C}(x)$-class function f, defined over $\mathbb{Z}_2$, sequence $\{x_i\}$ is generated by $x_0 \in \mathbb{Z}_2, x_{i+1} = f(x_i) = \cdots = f^i(x_0)$.Fixed any $n \geq 5$, we have*

$$x_{i+2^{j-1},j} = x_{i,j} + x_{i,j-1} + ajA_{i,2} + a(j-1) + b \bmod 2 \ (3 \leq j \leq n-1) \tag{53}$$

$\{A_{i,2}\}$ is a the sequence of period 4.So,

$$\begin{aligned} x_{i+2^{j-1},j} &= x_{i,j} + x_{i,j-1} + a + b \bmod 2, (aj \equiv 0 \bmod 2) \quad (54) \\ x_{i+2^{j-1},j} &= x_{i,j} + x_{i,j-1} + a + b + 1 \bmod 2, (aj \equiv 1 \bmod 2) \quad (55) \end{aligned}$$

Since to the sequence$\{x_i\}$ geberated by ergodic T-function, we know that $x_{i+2^j,j} \equiv x_{i,j} + 1 \bmod 2$, for all $i = 0, 1, 2, \ldots$.So

$$x_{i+1+2^j,j} + x_{i+2^j,j} + x_{i+1,j} + x_{i,j} \equiv 0 \bmod 2 \tag{56}$$

is the characteristic polynomial of the j-th coordinate sequence. Then combine (53)(54)(55)(56), we can get many indentities about the coordinate sequence., for example, (53)+(56), we get

$$x_{i+1+2^j,j}+x_{i+2^j,j}+x_{i+2^{j-1},j} \equiv x_{i+1,j}+x_{i,j-1}+ajA_{i,2}+a(j-1)+b \bmod 2 \tag{57}$$

and so on.

7 Conclusion

In theorem [2], we first give a proof that translate the ergodic condition for $\mathcal{C}(x)$-class function represented by falling factorial series to its power series representation. Then, we use it to deduce that Jin-Song Wang and Wen-Feng Qi's result on transitive polynomial T-function is a special case of our ergodic $\mathcal{C}(x)$-class function. Next, use Anashin's result, we give a number formula for polynomial type T-functions defined on $\mathbb{Z}/2^n\mathbb{Z}$, whose degree are not exceed m, and transitive(single-cycle) on all $\mathbb{Z}/2^k\mathbb{Z}, k \geq 2$,i.e theorem [3], then combine with Larin's result [6], we give the number formula for non-polynomial single-cycle T-functions on $\mathbb{Z}/2^n\mathbb{Z}$, and easily caculate the rate of single-cycle polynomial T-functions in all single-cycle T-functions on $\mathbb{Z}/2^n\mathbb{Z}$, i.e theorem [4]; using proposition [6], we deduce the least degree m that all the single-cycle polynomial transformations can be expressed as the polynomials that degree does not exceed m over $\mathbb{Z}/2^n\mathbb{Z}$,(n is fixed), i.e. theorem[5], and caculate some value of m for some small n. At last, for the close relation between $\mathcal{C}(x)$-class function and polynomial function, we generalized Jin-Song Wang and Wen-Feng Qi's result of linear equation over single cycle polynomial T-function to linear equation over ergodic $\mathcal{C}(x)$-class function.

Actually, we can generalized corresponding result to more general function class, i.e. $\mathcal{B}(x)$-class function. $f(x) \in \mathcal{B}(x)$ if and only if $f(x) = \sum_{i=0}^{\infty} b_i x^{\underline{i}}$, $(b_i \in \mathbb{Z}_p)$. In other words,

$$\mathcal{B}(x) = \{\sum_{i=0}^{\infty} a_i \binom{x}{i} : \frac{a_i}{i!} \in \mathbb{Z}_p; i = 0, 1, 2, \ldots\}$$

On $\mathbb{Z}/2^n\mathbb{Z}$, as a function, in force of a criterion for convergence of Mahler interpolation series, i.e. $\overset{p}{\lim\limits_{i\to\infty}} a_i = 0$, series from $\mathcal{B}(x)$ are uniformly convergent on $\mathbb{Z}_p$ and thus define uniformly continuous functions on $\mathbb{Z}_p$.And we have: [1] A $\mathcal{B}$-function (and thus a $\mathcal{C}$-function) f is measure-preserving if and only if f is bijective modulo p^2. The function f is ergodic if and only if f is transitive modulo p^2 whenever $p \notin \{2, 3\}$, or modulo p^3 whenever $p \in \{2, 3\}$.As power-series expression is more convenient to caculate, so we use two kinds Stirling numbers to translate $\mathcal{B}$-function from falling factorial series to power-series, and discuss our problem. Further result will be followed.

References

[1] Vladimir Anashin and Andrei Khrennikov, Applied Algebraic Dynamics, de Gruyter Expositions in Mathematics, vol. 49. 2009

[2] Jin-Song Wang and Wen-Feng Qi, Linear Equation on Polynomial Single Cycle T-Functions, Information Security and Cryptology: Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5, 2007, Revised Selected Papers, pages 256–270, 2008. 5.

[3] W.H.Schikhof, Ultrametric caculus, Cambridge University Press, 1984

[4] R. L. Graham, D. E. Knuth, and O. Patashnik. Concrete Mathematics: A Foundation for Computer Science. Addison–Wesley, Reading., Ma., second edition, 1998.

[5] Wenying Zhang and Chuan-Kun Wu, The Algebraic Normal Form, Linear Complexity and k-Error Linear Complexity of Single-Cycle T-Function, G. Gong et al. (Eds.): SETA 2006, LNCS 4086, pp. 391–401, 2006.

[6] M. V. Larin. Transitive polynomial transformations of residue class rings, Discrete Mathematics and Applications, 12(2):141–154, 2002.

[7] H. Molland and T. Helleseth, Linear Properties in T-Functions, IEEE Transactions On Information Theory, Vol. 52, No. 11, November 2006

[8] Ming-shu Tan, Combinatorial sequence and matrix (in Chinese), Science press, 2008.