2-Adic Complexity of Sequences Generated by T-Functions

Yan Wang, Xueming Ren, Shunbo Li, Song Zhao
(Corresponding author: Yan Wang)

Department of Mathematics, Xi'an University of Architecture and Technology
13, YanTa Road, Xi'an 710055, China
(Email: lanse-wy@163.com)

(Received July 12, 2017; revised and accepted Dec. 8, 2017)

Abstract

Single cycle T-functions are cryptographic primitives which can generate maximum periodic sequences. 2-Adic complexity of a sequence measures the difficulty of outputting a binary sequence using a feedback with carry shift register. Based on the special properties of single cycle T-functions, this paper investigates the 2-adic complexity of sequences generated by single cycle T-functions from the kth coordinate sequence to the state output sequence using the primality of Fermat number. It is shown that the state output sequence of a T-function is far from high 2-adic complexity.

Keywords: 2-Adic Complexity; Fermat Number; Sequence; T-Function

1 Introduction

The security of a stream cipher depends on the unpredictability of the pseudo-random bit sequence. To verify the pseudo-randomness of a sequence, criterions of pseudo-random sequence are proposed such as linear complexity, autocorrelation, 2-adic complexity and so on. In which 2-adic complexity of a sequence is used to measure how large a feedback with carry shift registers (FCSRs) is required to output a sequence.

Triangular functions (T-functions) are cryptography primitives proposed by Klimov and Shamir [7] which are built with help of fast arithmetic and Boolean operations wildly available on high-end microprocessors or on dedicated hard ware implementations. All the Boolean operations and most of the numeric operations in modern processors are T-functions, and their compositions are also T-functions. The main application of a single cycle mapping is in the construction of synchronous stream ciphers. Single cycle T-functions have some advantages as having 0 as its initial state, reaching the maximum length and having high efficiency in software, and they are suggested be new primitive of stream cipher, and also in block cipher and Hash functions to be the substitution of Linear Feedback Shift Register (LFSR).

Sequences generated by single cycle T-function are studied from the point of cryptographic criterion. The autocorrelation property of coordinate sequences is studied by Kolokotronis and Wang [8,14], and the results show that such sequence is not so pseudorandom as people expected. Linear complexity of sequences generated by single cycle T-function has been discussed in [1, 9, 15–17], which all show sequences generated by single cycle T-function have quite high linear complexity. As for 2-adic complexity of a sequence, Dong [3] studied the k-error 2-adic complexity of a binary sequence of a period p^n. Anashin [2] present a new criteria for a T-function to be bijective or transitive. Jang and Jeong *et al.* [4] give a characterization of 1-Lipschitz functions on $F_q[T]$ in terms of the van der Put expansion and use this result to give sufficient conditions for measure-preserving 1-Lipschitz function on $F_q[T]$ in terms of the three well known bases, Carlitz polynomials, digit derivatives and digit shifts. Sopin [12] presented the criteria of measure-preserving(Haar) for p^k-Lipschitz maps on the cartesian power of the ring of p-adic integers, where k is any natural of zero and p is an arbitrary prime. Sattarov [11] investigate the behavior of trajectory of a $(3, 2)$-rational p-adic dynamical system in complex p-adic field $\mathbb{C}_p$.

This paper investigated the 2-adic complexity of sequences generated by single cycle T-function, which refers the k-th coordinate sequence, the state output sequence by utilizing the properties of Fermat number.

The paper is organized as follows. Section 2 provides the basis concept of T-function, feedback with carry shift register (FCSRs), and some properties needed in our deduction. Section 3 analysis the 2-adic complexity of two types sequences generated by single cycle T-functions. Concluding remarks are given in Section 4.

2 Background

2.1 T-functions and Their Generating Sequences

Let $F_2 = \{0, 1\}$ be the finite field with two elements and integer n denote the word size. An n length single word $x = (x_0, x_1, \cdots, x_{n-1})$ is the vector in F_2^n which is the nth dimensional vector space over F_2.

Definition 1. *[7] Let $\underline{x} \in {F_2}^{m\times n}$, $\underline{y} \in {F_2}^{l\times n}$, and $\underline{x} = (x_0, x_1, \cdots, x_{m-1})^T$, $\underline{y} = (y_0, y_1, \cdots, y_{l-1})^T$, where $x_i = (x_{i,0}, x_{i,1}, \cdots, x_{i,n-1}) \in F_2^n$, $y_i = (y_{i,0}, y_{i,1}, \cdots, y_{i,n-1}) \in F_2^n$. Let $f : F_2^{m\times n} \to F_2^{l\times n}$ satisfies $f(\underline{x}) = \underline{y}$. If the ith row of the output $\underline{y}$ of f only depends on the $0, 1, \cdots, i$th row of input $\underline{x}$, we call f a T-function. When $m = l = 1$, we call f a single word T-function, otherwise a multiword T-function.*

Klimov and Shamir [7] have proved that every primitive operation which include negation, complementation, addition, subtraction, multiplication, XOR, and, and or, is a T-function. And an example of single cycle T-function as $x_i = x_{i-1}^2 \vee C + x_{i-1} \bmod 2^n$ is given, where $x_i \in Z, 0 \leqq x_i \leqq 2^n$ and $C = \ldots 101_2$ or $\ldots 111_2$.

Let T-function $f : F_2^n \to F_2^n$ be the state transition function, that is $x_i = f(x_{i-1})$. The sequence $\{x_i\}_{i\geq 0}$ is called the state output sequence of f. If the state sequence $\{x_i\}_{i\geq 0}$ of f has minimal period $N = 2^n$, f is called single cycle. Clearly, a single cycle T-function can produce a sequence with the maximal period sequence for n-bit words.

The sequence $\{x_{i,k}\}_{i\geq 0}(0 \leq k \leq n)$ generated by the kth bit of x_i is called the kth coordinate sequence of f. Following from [8], the kth coordinate has a period of $N_k = 2^{k+1}$, and satisfies

$$x_{i+2^k,k} = x_{i,k} \oplus 1.$$

This property exposed a disadvantage of T-function that the effective period of $\{x_{i,k}\}_{i\geq 0}$ is 2^k, a method of solving the problem is proposed in [8].

T-function can also be represented by vectorial Boolean function such as $f(x) = (f_0(x), f_1(x), \cdots, f_{n-1}(x))$, where each $f_k(x)(0 \leq k < n)$ is called the kth coordinate Boolean function which only depends on the first k bits of x. By the definition of T-function, the output of the kth coordinate Boolean is just the kth coordinate sequence of $\{x_i\}_{i\geq 0}$.

We want to make some observation about the properties of the sequences created by single cycle T-functions.

2.2 2-Adic Complexity

Since the security of traditional stream ciphers LFSR based is called into question, Goresky and Klapper proposed the feedback with carry shift register (FCSR) [5] which is similar to linear feedback shift register (LFSR) but with carry from one state to another.

An FCSR is determined by r coefficients $q_1, q_2, \cdots, q_r$ with $q_i \in \{0, 1\}, i = 1, 2, \cdots, r$, and an initial memory integer m_{r-1} which can be any integer. If the contents of the register at any given time are $(a_{n-1}, a_{n-2}, \cdots, a_{n-r+1}, a_{n-r})$ where $a_i \in \{0, 1\}, i = n-1, \cdots, n-r$, and the memory integer is m_{n-1}, then the operation of the shift register is defined as follows [6]:

A1: Form the integer sum $\delta_n = \sum_{k=1}^{r} q_k a_{n-k} + m_{n-1}$;

A2: Shift the contents one step to the right, outputting the rightmost bit a_{n-r};

A3: Place $a_n = \delta_n(\bmod 2)$ into the leftmost cell of the shift register;

A4: Replace the memory integer m_{n-1} with $m_n = (\delta_n - a_n)/2 = \lfloor \delta_n/2 \rfloor$.

Lemma 1. *[13] Let $\underline{x}$ be an eventually periodical sequence. Then $\alpha = \sum_{i=0}^{\infty} x_i 2^i$ is equal to p/q the quotient of p, q, where q is the connect number of the FCSR generating $\underline{x}$. Moreover, $\underline{x}$ is strictly periodical if and only if $1 \leq \alpha \leq 0$.*

Lemma 1 shows that every periodical sequence can be generated by an FCSR.

Let $\underline{x}$ be an eventually periodical binary sequence. If q is the connect number of FCSR generating $\underline{x}$, then q is called the connect number of $\underline{x}$. The following lemma can be got for the connect number of a sequence $\underline{x}$.

Lemma 2. *[13] Let $\underline{x}$ be generated by an FCSR, and q be the connect number of $\underline{x}$. Then $\underline{x}$ is an eventually periodical sequence and there exist an integer p such that $\alpha = \sum_{i=0}^{\infty} x_i 2^i = p/q$.*

Lemma 3. *[13] Let $\underline{x}$ be a strictly periodical sequence, then the minimum connect number $q_{\min}$ of $\underline{x}$ satisfies $q_{\min} \leq 2^{\mathrm{T}} - 1$.*

In this paper, we are interested in whether the bound is tight.

The same as the linear complexity, the 2-adic complexity of a sequence is intended to measure how large an FCSR is required to output the sequence.

Definition 2. *[13] Let $\underline{x}$ is a eventually binary sequence, $\sum_{i=0}^{\infty} x_i 2^i = p/q$, where $\gcd(p, q) = 1$. The real number $\phi_2(\underline{x}) = \log_2(\Phi(p, q))$ is called the 2-adic complexity of $\underline{x}$, where $\Phi(p, q) = \max(|p|, |q|)$.*

Actually, if a binary sequence s is strictly periodic, then its 2-adic complexity is clearer. The following corollary can be easily obtained.

Corollary 1. *[13] Let $\underline{x}$ be a strictly periodical binary sequence with the minimum connect number q. Then the 2-adic complexity of $\underline{x}$ is $\phi_2(\underline{x}) = \log_2 q$.*

Definition 3. *Let $\underline{x}$ be an FCSR sequence with connect number q and period T. $\underline{x}$ is called maximum period FCSR sequence, or l-sequence, if $T = \varphi(q)$ where $\varphi(q)$ is Euler function value of q.*

If $\underline{x}$ is a l-sequence with connect number q, then $ord_q(2) = \varphi(q)$ [6], and $q = p^e$ for some prime p and integer e, thereby $T = \varphi(q) = p^{e-1}(p-1)$.

3 Main Results

3.1 2-Adic Complexity of the kth Coordinate Sequence

In this section, 2-adic complexity of periodic sequences generated by single cycle T-function are discussed.

Lemma 4. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function with state sequence $\{x_i\}_{i\geq 0}$. Then the minimum connect integer $q_{\min}$ of the kth $(0 < k < n)$ coordinate sequence satisfies $q_{\min} \leq 2^{2^{k+1}} - 1$.*

Proof. This result can be proved according to the fact that the kth coordinate sequence have a period of 2^{k+1} and Lemma 3. □

Theorem 1. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function. Denote by s_k the kth coordinate output sequence. Then the 2-adic complexity $\phi_2(s_k) = \log_2 F_k$ when $k = 0, 1, 2, 3, 4$, where F_k is the kth Fermat Number $2^{2^k} + 1$.*

Proof. Denote the elements of s_k as $x_i, i = 0, 1, 2, \cdots$. By Lemma 2 and Lemma 4, for the sake of the 2-adic complexity of the kth coordinate sequence, we need to discuss

$$\begin{aligned}\sum_{i=0}^{\infty} x_i 2^i &= \frac{\sum_{i=0}^{T-1} x_i 2^i}{1-2^T} \\ &= -\frac{\sum_{i=0}^{2^{k+1}-1} x_i 2^i}{2^{2^{k+1}}-1} \\ &= -\frac{\sum_{i=0}^{2^{k+1}-1} x_i 2^i}{(2^{2^k}-1)(2^{2^k}+1)} \qquad (1)\end{aligned}$$

From the property of Single cycle T-function, the numerator can be expressed as

$$\begin{aligned}\sum_{i=0}^{2^{k+1}-1} x_i 2^i &= \sum_{i=1}^{2^k-1} [x_{i,k} \cdot 2^i + x_{i+2^k,k} \cdot 2^{i+2^k}] \\ &= \sum_{i=1}^{2^k-1} [x_{i,k} \cdot 2^i + (x_{i,k} \oplus 1) \cdot 2^{i+2^k}] \quad (2)\end{aligned}$$

Since $\{x_i, x_i \oplus 1\} = \{0, 1\}$, the above sum means choosing a number from every column in the following numbers and then adding them together:

1	2	4	$\ldots$	2^i	$\ldots$	2^{2^k-1}
2^{2^k}	$2 \cdot 2^{2^k}$	$4 \cdot 2^{2^k}$	$\ldots$	$2^i \cdot 2^{2^k}$	$\ldots$	$2^{2^k-1} \cdot 2^{2^k}$

Denote that $S = \{i | x_{i+2^k,k} = 1, 0 \leq i \leq 2^k - 1\}$ with cardinality m. So S also can be $\{i_1, i_2, \cdots, i_m\}$, and $x_{i,k} = 0, i \in S$. Then the sum in Equation(2) will be:

$$\begin{aligned}&\sum_{i=1}^{2^k-1} [x_{i,k} \cdot 2^i + (x_{i,k} \oplus 1) \cdot 2^{i+2^k}] \\ =& \sum_{i=1}^{2^k-1} (1 \cdot 2^i) + \sum_{i=1, i\in S}^{2^k-1} x_{i,k} \cdot (2^{i+2^k} - 2^i)] \\ =& (2^{2^k} - 1) + (2^{2^k} - 1)(2^{i_1} + 2^{i_2} + \ldots + 2^{i_m}) \\ =& (2^{2^k} - 1)(1 + 2^{i_1} + 2^{i_2} + \ldots + 2^{i_m}).\end{aligned}$$

So the right fraction term in Equation (1) will be

$$\begin{aligned}&\frac{(2^{2^k} - 1)(1 + 2^{i_1} + 2^{i_2} + \ldots + 2^{i_m})}{(2^{2^k} - 1)(2^{2^k} + 1)} \\ =& \frac{1 + 2^{i_1} + 2^{i_2} + \ldots + 2^{i_m}}{2^{2^k} + 1} \qquad (3)\end{aligned}$$

Denote the kth Fermat number as F_k. For the case of 2-adic complexity of the kth coordinate sequence, the question becomes whether the kth Fermat number is a composite number.

From [10], the first five Fermat number $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ and $F_4 = 65537$ are indeed prime.

As far as the numerator, since $1 + 2^{i_1} + 2^{i_2} + \cdots + 2^{i_m} < 2^{2^k} + 1$, we can deduce that the 2-adic complexity of the kth coordinate sequence for all the single cycle T-function is $\log_2 F_k$ when $k = 0, 1, 2, 3, 4$, and they are $\log_2 3, \log_2 5, \log_2 17, \log_2 257, \log_2 65537$. □

Theorem 2. *Let $f : {F_2}^n \to {F_2}^n$ be single cycle T-function, s_k be the kth coordinate output sequence of f, $T = 2^{k+1}$ be the period of s_k, and q be the minimum connect integer. Then, $\phi_2(s_k) < T \leq \varphi(q) < 2^T - 2$ for $k = 0, 1, 2, 3, 4$, where φ is the Euler function.*

Proof. Firstly, by Theorem 1,

$$\begin{aligned}\phi_2(s_k) &= \log_2(2^{2^k} + 1) \\ &< \log_2 2^{2^k} \cdot 2^{2^k} \\ &= \log_2 2^{2^{k+1}} \\ &= 2^{k+1} \\ &= T.\end{aligned}$$

Since $\varphi(q) = 2^{2^k}$ and $T = 2^{k+1}$, we have $T \leq \varphi(q)$, where the equation is established if and only if $k = 0, 1$. When $k = 0, 1, 2, 3, 4$, $q = 2^{2^k} + 1$ is prime, $\varphi(q) = q - 1$, and by Lemma 3, $q < 2^T - 1$, we have $\varphi(q) < 2^T - 2$. □

Thus, the kth coordinate sequence is an l-sequence when $k = 0, 1$.

As for $5 \leq k \leq 23$, it has been proved that F_k is composite [10], and also, for $k \geq 2$, the factors of F_k are of the form $m2^{k+2} + 1$. There still no new Fermat prime number was found.

Theorem 3. *Let $f : F_2{}^n \rightarrow F_2{}^n$ be single cycle T-function, s_k be the kth coordinate output sequence of f, and $F_k = p_1 p_2 \cdots p_t$, where $k \geq 5$ and $p_i, i = 1, 2, \cdots, t$ is prime. Then,*

1) *If the bottom half of s_k is just the binary number of some p_i, then the 2-adic complexity of s_k is $\log_2 \frac{F_k}{p_i}$;*
2) *If the bottom half of s_k has factors $\{p_{j_1}, p_{j_2}, \cdots, p_{j_u}\} \subset \{p_1, p_2, \cdots, p_t\}$, then the 2-adic complexity of s_k is $\log_2 \frac{F_k}{p_{j_1} p_{j_2} \cdots p_{j_u}}$.*

Proof. If $k \geq 5$, and F_k has a prime factorization $F_k = p_1 p_2 \cdots p_t$, then the 2-adic complexity depends on the factorization of the numerator in Equation (3). Since the bottom half of sequence s_k is just the exponential sequence of the numerator in Equation (3), and Equation (3) will become $\frac{1}{F_k / p_i}$. And it will become $\frac{1}{F_k / p_{j_1} p_{j_2} \cdots p_{j_u}}$ when the bottom half of s_k has factors $\{p_{j_1}, p_{j_2}, \cdots, p_{j_u}\} \subset \{p_1, p_2, \cdots, p_t\}$. □

Theorem 4. *Let $f : F_2{}^n \rightarrow F_2{}^n$ be single cycle T-function, s_k be the kth ($k \in Z, 5 \leq k \leq 13$) coordinate output sequence of f, $T = 2^{k+1}$ be the period of s_k, and q be the minimum connect integer. Then, $\phi_2(s_k) < T < \varphi(q) < 2^T - 2$, where $\varphi(q)$ is Euler function value of q.*

Proof. We just need to verify that $T < \phi(q)$ for ($k \in Z, 5 \leq k \leq 13$). We need to check the factorization of F_k for ($k \in Z, 5 \leq k \leq 13$). Since

$$\begin{aligned}
F5 &= 641 \times 6700417 \\
F6 &= 274177 \times 67280421310721 \\
F7 &= 59649589127497217 \times 5704689200685129054721 \\
F8 &= 1238926361552897 \times 93461639715357977769163 \\
&\quad 558199606896584051237541638188580280321 \\
F9 &= 2424833 \times 7455602825647884208337395736 \\
&\quad 200454918783366342657 \times 74164006262753 \\
&\quad 080152478714190193747405994078109751902390 \\
&\quad 558213161444157595047000809281871169394 0737 \\
F10 &= 45592577 \times 6487031809 \times 4659775785220018 \\
&\quad 543264560743076778192897 \times P252 \\
F11 &= 319489 \times 974849 \times 167988556341760475137 \\
&\quad \times 3560841906445833920513 \times P564 \\
F12 &= 114689 \times 26017793 \times 63766529 \times 190274191361 \\
&\quad \times 1256132134125569 \times 5686306475353569551 \\
&\quad 69033410940867804839360742060818433 \\
&\quad \times C1133 \\
F13 &= 710954639361 \times 2663848877152141313 \\
&\quad \times 3603109844542291969 \\
&\quad \times 319546020820551643220672513 \\
&\quad \times C2391.
\end{aligned}$$

Every minimum connect number is equal to one or a sum of the factors, compare them with $T = 2^{k+1}$ we can verify the inequality. □

Actually, when $14 \leq k \leq 23$, we have known that F_k is a composite number while the factors is unknown, we have the conjecture that the above inequality still holds.

From Theorem 1 and Theorem 3, we know that 2-adic complexity of the kth coordinate sequence is far out of reach the maximum value.

3.2 2-Adic Complexity of the State Output Sequence

Theorem 5. *Let $f : F_2{}^n \rightarrow F_2{}^n$ be single cycle T-function with state sequence $S = x_{0,0}, x_{0,1}, \cdots, x_{i,j}, \cdots, x_{n-1,2^n-1}$, $i = 0, 1, \cdots, n-1$, $j = 0, 1, \cdots, 2^n - 1$ which has a period of $n \cdot 2^n$. Then s_t has the maximum 2-adic complexity $\log_2 2^{n \cdot 2^{n-1}+1}$.*

Proof. For the state output sequence, check the following fraction:

$$\sum_{i=0}^{\infty} x_i 2^i = \frac{\sum_{i=0}^{T-1} x_i 2^i}{1 - 2^T} = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{2^n-1} x_{i,j} 2^{j + i \cdot 2^n}}{1 - 2^T}$$

	$n-1$	$\ldots$	2	1	0
0	$x_{0,n-1}$	$\ldots$	$x_{0,2}$	$x_{0,1}$	$x_{0,0}$
1	$x_{1,n-1}$	$\ldots$	$x_{1,2}$	$x_{1,1}$	$x_{1,0}$
$\vdots$					
$2^n - 1$	$x_{2^n-1,n-1}$	$\ldots$	$x_{2^n-1,2}$	$x_{2^n-1,1}$	$x_{2^n-1,0}$

If $x_{i,j} = 1$, the first half of the sum in numerator becomes

$$\sum_{i=0}^{n-1} \sum_{j=0}^{2^{n-1}-1} 1 \cdot 2^{j + i \cdot 2^n} = 2^{n \cdot 2^{n-1}} - 1$$

Denote the location of nonzero in the last bottom half of S by $t_1, t_2, \cdots, t_u$, then the last half of the sum in numerator is

$$(2^{n \cdot 2^{n-1}} - 1)(2^{t_1} + 2^{t_2} + \cdots + 2^{t_t})$$

So the whole sum in numerator is

$$(2^{n \cdot 2^{n-1}} - 1)(1 + 2^{t_1} + 2^{t_2} + \cdots + 2^{t_t})$$

and Equation 3.2 will be

$$\frac{1 + 2^{t_1} + 2^{t_2} + \cdots + 2^{t_t}}{1 + 2^{n \cdot 2^{n-1}}}$$

So s_t has the maximum 2-adic complexity $\log_2 2^{n \cdot 2^{n-1}+1}$. □

We can verify when $n = 2$, $2^{n\cdot 2^{n-1}+1}$ is prime, and when $n = 3, 4, 5$, $2^{n\cdot 2^{n-1}+1}$ is composite number. When n is more lager, we can have the following corollary:

Corollary 2. *Both the kth coordinate sequence and the state output sequence of single cycle T-function have maximum 2-adic complexity as* $\log_2(2^{T/2}+1)$, *where* T *is the period of the sequence.*

Corollary 3. *Let* $f(x) : F_2^n \to F_2^n$ *be a single cycle T-function. Then the maximum 2-adic complexity of its kth coordinate sequence and state output sequence have approximate value* $T/2$ *where* T *is the period of the sequence.*

Proof. This result can be deduced by $\log_2 2^{n\cdot 2^{n-1}+1} \approx \log_2 2^{n\cdot 2^{n-1}} = T/2$. □

Compare to the m-sequence [13], the single cycle T-function sequence can have the same well properties when we choose the coordinate sequence.

Corollary 4. *Let* s *be the state output sequence of a single cycle T-function* f *with period* T, *2-adic complexity* $\phi_2(s)$, *minimum connect number* q. *Then* $\varphi(q) < 2^T - 2$, *and*

$$\phi_2(s_k) < T < \varphi(q) < 2^T - 2$$

holds when f *is defined in* $F_2, F_2^2, F_2^4, F_2^5, F_2^6, F_2^7, F_2^8, F_2^{16}, F_2^{32}$.

Proof. Since the connect number $\varphi(q) \le q-1$ for all prime or composite number q, we have $\varphi(q) < q-1 < 2^T - 2$. By Corollary T3, $\phi_2(s_k) \le T/2$, so $\phi_2(s_k) < T$. For $f : F_2{}^n \to F_2{}^n$ where $n = 1, 2, 4, 5, 6, 7, 8, 16, 32$, we can verify that the minimum vale of $\varphi(q)$ is less than $n \cdot 2^n$, so $\phi_2(s_k) < T < \varphi(q) < 2^T - 2$. □

4 Conclusions

Since it is suggested that a single cycle T-function can be the substitution of linear feedback shift register for its long cycle and nonlinearity structure. Comparison between m-sequence and sequences generated by single cycle T-function become and interesting problem. Tian Tian shows 2-adic complexity of the m-sequence attains the maximum in [13]. And in [15], it is shown that the sequences generated by single cycle T function have high linear complexity. In this paper, 2-adic complexity of the kth coordinate sequence, the state output sequence generated by a single cycle T-function is studied. It is shown that these two sequences are not as pseudo-random as m-sequence in the respect of 2-adic complexity.

Acknowledgments

This study was supported by the Natural Science Basic Research Plan in Shaanxi Province of China (No. 2014JQ1027), Basic Research Foundation of Xi'an University of Architecture and Technology (No. JC1416), the National Natural Science Foundation of China (No. 11471255), and the Talents Foundation of Xi'an University of Architecture and Technology (No.RC 1338).

References

[1] V. Anashin and A. Khrennikov, "Applied algebraic dynamics," *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 2, no. 4, pp. 360–362, 2010.

[2] V. Anashin, A. Khrennikov, and E. Yurova, "T-functions revisited: New criteria for bijectivity/transitivity," *Designs Codes and Cryptography*, vol. 71, no. 3, pp. 383–407, 2014.

[3] L. H. Dong and Y. P. Hu, "Computing the k-error 2-adic complexity of a binary sequence of period pn," *International Journal of Computer Science and Network Security*, no. 3, pp. 66–70, 2006.

[4] Y. Jang, J. Sangtae, and C. L. Li, "Criteria of measure-preservation for 1-lipschitz functions on f q [[t]] in terms of the van der put basis and its applications," *Finite Fields and Their Applications*, vol. 37, pp. 131–157, 2016.

[5] A. Klapper and M. Goresky, "2-adic shift registers," in *Fast Software Encryption*, pp. 174–178, 1994.

[6] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *Journal of Cryptology*, vol. 10, no. 2, pp. 111–147, 1997.

[7] A. Klimov and A. Shamir, "A new class of invertible mappings," in *The 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES '02)*, pp. 470–483, 2003.

[8] N. Kolokotronis, "Cryptographic properties of nonlinear pseudorandom number generators," *Designs Codes and Cryptography*, vol. 46, pp. 353–363, 2008.

[9] X. Ma, T. Yan, D. Zhang, and Y. Liu, "Linear complexity of some binary interleaved sequences of period 4n," *International Journal of Network Security*, vol. 18, no. 2, pp. 244–249, 2016.

[10] P. B. Richard, "Factorization of the tenth and eleventh fermat numbers," *Mathematics of Computation*, vol. 68, no. 154, pp. 627–630, 2000.

[11] I. A. Sattarov, "p-adic (3, 2)-rational dynamical systems," *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 7, no. 1, pp. 39–55, 2015.

[12] V. Sopin, "Criteria of measure-preserving for p k-lipschitz mappings," *P-Adic Numbers, Ultrametric Analysis, and Applications*, vol. 7, no. 1, pp. 76–79, 2015.

[13] T. Tian and W. F. Qi, "2-adic complexity of binary m-sequences," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 450–454, 2010.

[14] Y. Wang, Y. P. Hu, S. B. Li, and Y.Yang, "Autocorrelation of sequences generated by single cycle t-functions," *China Communications*, vol. 8, no. 5, pp. 144–150, 2011.

[15] Y. Wang, Y. P. Hu, S. B. Li, and Y. Yang, "Linear complexity of sequence produced by single cycle t-function," *The Journal of China Universities of Posts and Telecommunications*, vol. 18, pp. 123–128, 2011.

[16] W. Y. Zhang and C. K. Wu, "The algebraic normal form, linear complexity and k-error linear complexity of single-cycle t-function," *Sequences and Their Applications (SETA'06)*, pp. 391–401, 2006.

[17] L. Zhao and Q. Y. Wen, "Linear complexity and stability of output sequences of single cycle t-function," *Journal of Beijing University of Posts and Telecommunications*, vol. 31, no. 4, pp. 62–65, 2008.

Biography

Yan Wang Ph.D., associate professor, Bachelor of Shaanxi Normal University in 2003, Ph. D. of Xi'an Electronic and Science University in 2012, visiting scholar of Ohio State University in 2015. Research direction is cryptography. Presided over 1 Shaanxi Natural Science Foundation Projection and 1 Natural Science Foundation of Shaanxi Education Department. Published more than 20 scientific research papers in important journals at home and abroad.

Xueming Ren Ph. D., second grade professor, Ph. D. supervisor, Ph. D. graduated from Chinese University Hong Kong. The main research areas are semigroup algebra theory and its applications. Presided over the completion of 7 National Natural Science Foundation Project and the Shaanxi Natural Science Foundation Projection. Published more than 80 scientific research papers in important journals at home and abroad, such as the "Journal of Algebra", "Communications in Algebra", "Semigroup Forum", "Chinese science", "Science Bulletin". These theses have been cited by many domestic and foreign colleagues in important academic journals. His research achievements have won the first prize of the Provincial Natural Science, the ministerial level scientific and technological progress third prize, and the Provincial Education Commission, science and technology progress second prize ones.

Shunbo Li Associate professor at School of Science, Xi'an University of Architecture and Technology, China. Received the Ph.D. degree in applied mathematics from Xidian University, Xi'an, China, in 2012. His research fields include information security theory and stream cipher. Published more than 20 scientific research papers in important journals at home and abroad.