Linear Complexity of Pseudorandom Sequence over Odd Characteristic Field

Chiaki Ogawa, Yasuyuki Nogami, Hiroto Ino, Satoshi Uehara, Robert Morelos-Zaragoza

Background

The pseudo random sequence for cryptographies and communication systems need to have some important features. Researching the pseudo random numbers with special characteristics is one of the important study for communication technology.

Previous work and Purpose

M-sequence + L-sequence

multi-value sequence

*including binary sequence

In the previous work, the multi-valued pseudo random sequence by combining the features of M-sequence and Legendre sequence has been proposed. The method of generating this sequence has mainly 4 steps. This sequence has important features of linear complexity and periodic autocorrelation. These features also have been researched in some previous works. This study focused on the profile of the linear complexity. It means that this work observes the linear complexities for each interval of the sequence.

Generating methods

1. Generating vectors

$$x^i \bmod f(x)$$

$f(x)$: primitive polynomial over F_p

The first is generating the maximum length vector sequence by using a primitive polynomial over finite field.

$$x^0 = 0x + 1$$
$$x^1 = 1x + 0$$
$$x^2 = 2x + 4$$
$$x^3 = 1x + 1$$
$$x^4 = 3x + 4$$
$$\vdots$$
$$x^{46} = 6x + 4$$
$$x^{47} = 2x + 3$$
$$x^{48} = 0x + 1$$

2. Vectors to Scalars

$$Tr(X) = \sum_{k=0}^{m-1} (X)^{p^k}$$

The second is mapping the vectors to multi-valued scalars by applying trace function.

$$\mathrm{Tr}(x^0) = 2$$
$$\mathrm{Tr}(x^1) = 2$$
$$\mathrm{Tr}(x^2) = 5$$
$$\mathrm{Tr}(x^3) = 4$$
$$\mathrm{Tr}(x^4) = 0$$
$$\vdots$$
$$\mathrm{Tr}(x^{46}) = 6$$
$$\mathrm{Tr}(x^{47}) = 3$$
$$\mathrm{Tr}(x^{48}) = 2$$

3. Calculating k-th power residue

$$(a/p)_k = a^{\frac{p-1}{k}} \bmod p$$

The third is applying k-th power residue symbol, which is the extended version of Legendre symbol, to map the scalars to k-valued sequence, where k is a certain prime number.

$$(2/7)_3 = 4$$
$$(2/7)_3 = 4$$
$$(5/7)_3 = 4$$
$$(4/7)_3 = 2$$
$$(0/7)_3 = 0$$
$$\vdots$$
$$(6/7)_3 = 1$$
$$(3/7)_3 = 2$$
$$(2/7)_3 = 4$$

4. Mapping

$$f_k(x) = \begin{cases} l \bmod p & \text{when } x = \varepsilon_k^l \\ 0 & \text{else} \end{cases}$$

ε_k: k-th primitive root

Finally, the number of the kind of $f_k(x)$ in this k-valued sequence within the period is clearly given, since the input for $f_k(x)$ is 0 or ε_k^l.

$$f_3(2^2) = 2$$
$$f_3(2^2) = 2$$
$$f_3(2^2) = 2$$
$$f_3(2^1) = 1$$
$$f_3(0) = 1$$
$$\vdots$$
$$f_3(2^0) = 0$$
$$f_3(2^1) = 1$$
$$f_3(2^2) = 2$$

Important features

① Period : The length of this sequence is $\lambda = \frac{k(p^m-1)}{p-1}$.

② Cyclical autocorrelation : This property gives period, similarity and etc.

③ Linear complexity : This is used for verification of difficulties of estimating sequence. **← focused**

Linear complexity

The linear complexity $\mathrm{LC}(S)$ is defined as follows.

$$\mathbf{LC}(\boldsymbol{S}) = \boldsymbol{\lambda} - \mathbf{deg}\left(\mathbf{gcd}\left(\boldsymbol{x}^{\boldsymbol{\lambda}} - \mathbf{1}, \boldsymbol{h_S}(\boldsymbol{x})\right)\right)$$

$$h_S(x) = \sum_{i=0}^{\lambda-1} s_i x^i$$

S : sequence, $S = \{s_i\}$

λ : the period of sequence

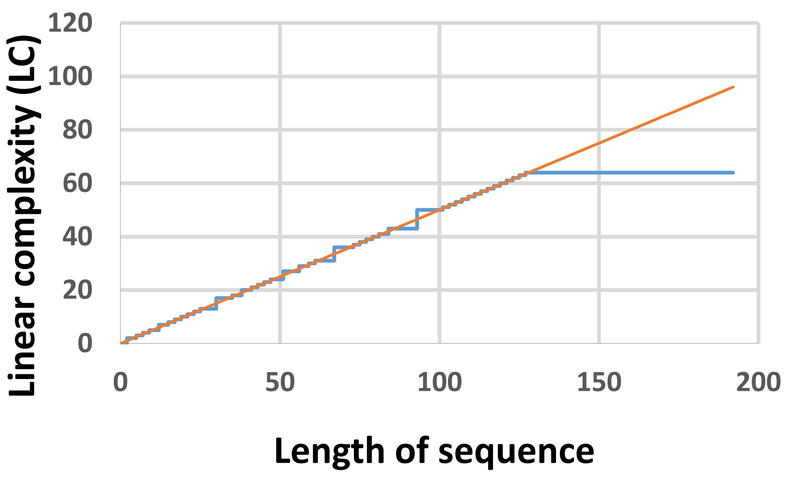
It is noted that $\gcd\left(x^{\lambda} - 1, h_S(x)\right)$ needs to be calculated over F_k

The pseudo random multi-valued sequence has the linear complexity $\frac{2(p^m-1)}{p-1}$ for the whole of the period λ.

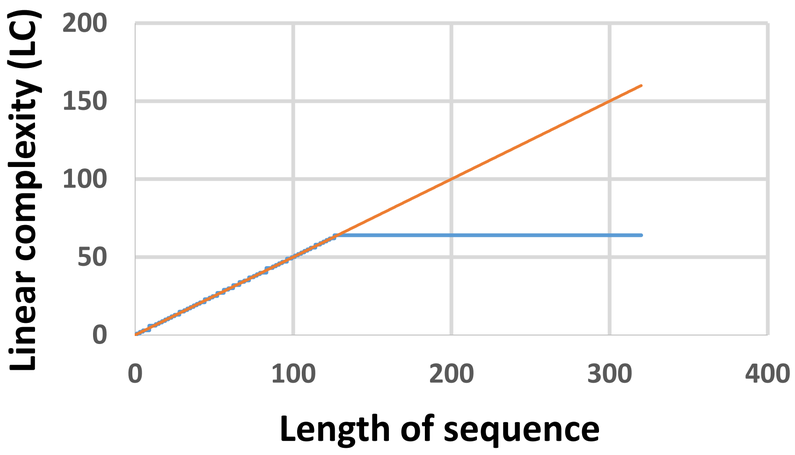
Linear complexity profile

To observe its linear complexity profile, this study applies Berlekamp-Massey algorithm. From the aspect of the specification of this algorithm, the possible maximum value of the linear complexity for each length will be indicated around the line which is described in graphs($\mathrm{LC} = {}^{n}/_{2}$). In fact, when the two sequences are fully observed, the linear complexity of a whole period will be obtained, thus the value appears at $n = 2\lambda$.

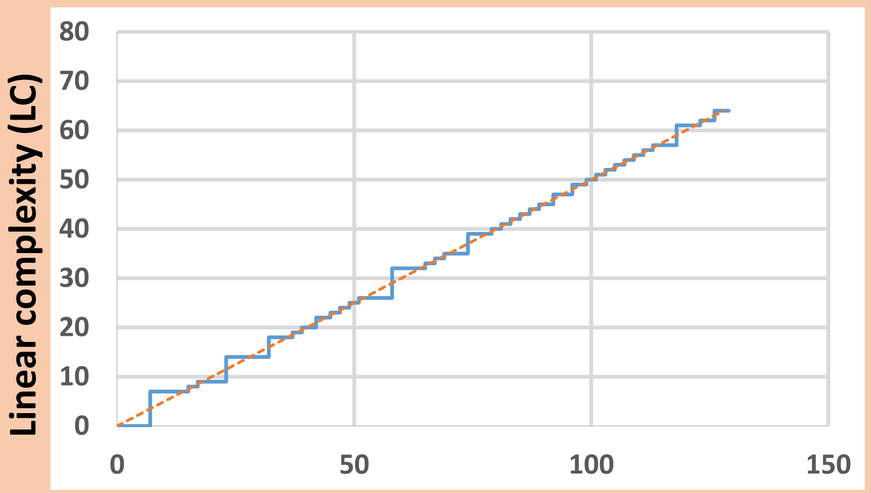
period $\lambda = 96$, $k = 3$



period $\lambda = 160$, $k = 5$



period $\lambda = 64$, $\boldsymbol{k = 2}$



From these results, the considered sequence will be suitable for the use of cryptographic systems when the parameter k is set as 2.

Conclusions and future works

According to the experimental observation of the linear complexity profile, it is found that the linear complexity for the every interval become around the possible maximum value when the parameter k is set as 2. It has been shown that this binary sequence has maximum difficulty of being estimated for every interval. Thus it can be said that this binary sequence is enough complicated and suitable for the use in cryptographic applications. As a future work, the mathematical proof of this property and evaluation of the cost of generating sequence based on the use in actual applications will be given.

This work was supported by JSPS KAKENHI Grantin-Aid for Scientific Research (A) Number 16H01723.