April 1, 2017

Multi-Valued Sequences Generated by Power Residue Symbols over Odd Characteristic Fields

Begum Nasima, *University of Asia Pacific*
Yasuyuki Nogami, *Okayama University*
Satoshi Uehara, *University of Kitakyushu*
Robert H Morelos-Zaragoza, *San Jose State University*

IEICE TRANS. FUNDAMENTALS, VOL.E100–A, NO.4 APRIL 2017

PAPER Special Section on Signal Design and Its Applications in Communications

Multi-Valued Sequences Generated by Power Residue Symbols over Odd Characteristic Fields

Begum NASIMA[†a)], **Yasuyuki NOGAMI**[††b)], **Satoshi UEHARA**[†††c)], ***Members***, ***and*** **Robert H. MOLEROS-ZARAGOZA**[††††d)], ***Nonmember***

SUMMARY This paper proposes a new approach for generating pseudo random multi-valued (including binary-valued) sequences. The approach uses a primitive polynomial over an odd characteristic prime field $\mathbb{F}_p$, where p is an odd prime number. Then, for the maximum length sequence of vectors generated by the primitive polynomial, the trace function is used for mapping these vectors to scalars as elements in the prime field. Power residue symbol (Legendre symbol in binary case) is applied to translate the scalars to k-value scalars, where k is a prime factor of $p-1$. Finally, a pseudo random k-value sequence is obtained. Some important properties of the resulting multi-valued sequences are shown, such as their period, autocorrelation, and linear complexity together with their proofs and small examples.

key words: *geometric sequence, multi-valued sequence, odd characteristic, primitive polynomial, Legendre symbol, trace*

1. Introduction

Pseudo random *binary* sequences such as maximum length sequence (M-sequence) [1] and Legendre sequence (L-sequence) [2] have been researched well since most of important properties are theoretically proven and they have many applications for control systems and cryptographies. The authors have proposed an approach to generate a pseudo random binary sequence by combining the features of M-sequence and L-sequence [3]. In brief, while M-sequence (resp. L-sequence) uses a primitive polynomial (resp. Legendre symbol), our previous work uses a primitive polynomial over an odd characteristic field to generate a maximum-length vector sequence, then applies the trace function to map the vectors to multi-valued scalars, and finally applies Legendre symbol to binarize the scalars. M-sequence and L-sequence are respectively characterized with the degree m of primitive polynomial and the characteristic p of the base field. On the other hand, the pseudo random binary sequences of [3] have two parameters p and m and a new variety of pseudo binary random sequences were successfully constructed for which some important properties such as their period, and auto-correlation, linear complexity have been theoretically proven. This result is extended here to the generation of pseudo random *multi-valued* sequences.

The pseudo random *multi-valued* sequence proposed in this paper is briefly introduced as follows. Let p be an odd characteristic and m be the degree of a primitive polynomial $f(x)$ over prime field $\mathbb{F}_p$. Then, $f(x)$ is able to generate a maximum length sequence over $\mathbb{F}_p$. Let ω be a root of $f(x) = 0$, a primitive element in $\mathbb{F}^*_{p^m}$. $\mathbb{F}^*_q$ denotes the multiplicative group of $\mathbb{F}_q$, that is $\mathbb{F}^*_q = \mathbb{F}_q - \{0\}$. Then the sequence,

$$\mathcal{S} = \{s_i\},\ s_i = \mathrm{Tr}\left(\omega^i\right),\ i = 0, 1, 2, \cdots, p^m - 2$$

is a maximum length sequence of period $p^m - 1$, where $\mathrm{Tr}(\cdot)$ is the trace function over $\mathbb{F}_p$. Based on this fact, the proposed approach applies the k-th *power residue symbol* for mapping the trace sequence $\mathcal{S}$ to the multi-valued sequence $\mathcal{T}$, where $\mathcal{T}$ consists of integers between 0 to $k-1$ and k needs to be a prime factor of $p-1$. Most of the previous works in this area are basically focused on *binary* sequences [4], [5]. On the other hand, this paper adapts power residue symbol for the mapping from $\mathcal{S}$ to $\mathcal{T}$, and it is shown that the obtained *multi-valued* sequences $\mathcal{T}$ has a period of $n = k(p^m - 1)/(p-1)$ and a typical periodic autocorrelation. This paper also discusses their linear complexity together with small examples. It is experimentally observed that the linear complexity of the sequence $\mathcal{T}$ becomes $2(p^m - 1)/(p-1)$ without any exceptions. Thus, the linear complexity does not depend on the parameter k while the period does. For the case of $m = 2$, the linear complexity is theoretically proven. Then, this paper shows some examples. We should note that the previous work in [3] is reduced to the case $k = 2$ of this paper. Even though there are a few papers in this area [6], [7], this paper shows a new variety of pseudo random *multi-valued* sequences.

Throughout this paper, p and q denote an odd prime number and its power $q = p^m$, respectively, where m is a natural number and mainly denotes extension degree. A *multi-valued* sequence in this paper means: a sequence that consists of integer coefficients between 0 to $k-1$, where k is a prime number such that k divides $p-1$. While the

Manuscript received July 8, 2016.
Manuscript revised November 28, 2016.

[†]The author is with Department of Computer Science and Engineering, University of Asia Pacific, 74/A, Green Road, Dhaka-1215, Bangladesh.
[††]The author is with Graduate School of Natural Science and Technology, Okayama University, Okayama-shi, 700-8530 Japan.
[†††]The author is with Graduate School of Environmental Engineering, The University of Kitakyushu, Fukuoka-shi, 808-0135 Japan.
[††††]The author is with Department of Electrical Engineering, San Jose State University, 1 Washington Square, San Jose, CA 95192-0084, USA.
a) E-mail: mail4nasima@gmail.com
b) E-mail: yasuyuki.nogami@okayama-u.ac.jp
c) E-mail: uehara@kitakyu-u.ac.jp
d) E-mail: R.Morelos-Zaragoza@IEEE.org
DOI: 10.1587/transfun.E100.A.922

focus of this paper is over an odd characteristic *prime* field $\mathbb{F}_p$ as the base field, the results hold over an arbitrary odd characteristic *extension* field as base field.

1.1 Contributions of This Paper

The main features of the pseudo random multi-valued sequence proposed in this paper are summarized as follows.

Theoretically proven

- period : $n = \dfrac{k(p^m - 1)}{(p-1)}$
- number of each value in one period
- periodic autocorrelation with k peaks
- linear complexity $\dfrac{2(p^m - 1)}{(p-1)}$ when $m = 2$

Experimentally observed for many cases

- linear complexity $\dfrac{2(p^m - 1)}{(p-1)}$ when $m \neq 2$

2. Preliminaries

This section presents a review of mathematical fundamentals such as primitive element, power residue symbol and its property, trace, dual basis, multi-valued sequence, autocorrelation of multi-valued sequence, and linear complexity. As previously noted, k is a prime factor of $p - 1$.

2.1 Primitive Element and Primitive Polynomial

It is well known that every finite field $\mathbb{F}_q$ has a primitive element that generates $\mathbb{F}_q^*$. In other words, let g be a generator, then every non-zero element can be expressed by its power g^i for $i = 0, 1, 2, \cdots, q-2$. The minimal polynomial of this generator is correspondingly called a primitive polynomial.

According to Fermat's little theorem, the following property between $\mathbb{F}_q$ and its base field $\mathbb{F}_p$ holds.

Property 1. *Let g be a generator of $\mathbb{F}_q^*$. Then $g^{(q-1)/(p-1)}$ is a non-zero element in prime field $\mathbb{F}_p$ that is also a generator of $\mathbb{F}_p^*$.* □

2.2 Power Residue Property and Its Symbol

For an arbitrary element a in $\mathbb{F}_p$, where p is an odd prime number, it is called *quadratic residue* (QR) in $\mathbb{F}_p$ if $a \neq 0$ and has square roots in $\mathbb{F}_p$. If it does not have any square roots in $\mathbb{F}_p$, it is called *quadratic non- residue* (QNR) in $\mathbb{F}_p$. Whether a is a quadratic residue is able to be examined by the exponentiation of $(p-1)/2$ in $\mathbb{F}_p$ and then Legendre symbol $\left(a/p\right)$ is defined as follows.

$$\left(a/p\right) = a^{(p-1)/2} = \begin{cases} 0 & \text{when } a = 0. \\ 1 & \text{when } a \text{ is a QR in } \mathbb{F}_p^* \\ p-1 & \text{when } a \text{ is a QNR in } \mathbb{F}_p^* \end{cases}. \quad (1)$$

It is extended for a prime factor k of $p - 1$. If $a \in \mathbb{F}_p$ is not equal to zero and has k-th power roots in $\mathbb{F}_p$, it is called k-th *power residue* (PR) in $\mathbb{F}_p$. If a does not have k-th power roots in $\mathbb{F}_p$, it is called k-th *power non-residue* (PNR) in $\mathbb{F}_p$. Then, let ϵ_k be a primitive k-th power root of unity in $\mathbb{F}_p$, k-th power residue symbol $\left(a/p\right)_k$ with the exponentiation of $(p-1)/k$ is similarly defined as follows.

$$\left(a/p\right)_k = a^{(p-1)/k} = \begin{cases} 0 & \text{when } a = 0. \\ 1 = \epsilon_k^0 & \text{when } a \text{ is a } k\text{-th PR in } \mathbb{F}_p^* \\ \epsilon_k^i \neq 1 & \text{when } a \text{ is a } k\text{-th PNR in } \mathbb{F}_p^* \end{cases}. \quad (2)$$

In the above equation, ϵ_k^i just means a certain power of ϵ_k, where $1 \leq i < k$. In the same way as Legendre symbol, the power residue symbol is generally used for checking whether a is a k-th PR in $\mathbb{F}_p$. In this paper, it is used to translate a trace sequence[†] over $\mathbb{F}_p$ to a k-valued sequence.

The following property of the k-th power residue symbol over $\mathbb{F}_p$ is known.

Property 2. *The number of k-th PRs and k-th PNRs in $\mathbb{F}_p^*$ are given by $(p-1)/k$ and $(k-1)(p-1)/k$ respectively.* □

Proof. Let g be a generator of $\mathbb{F}_p^*$. Then, a primitive k-th root ϵ_k of unity is represented by $g^{(p-1)/k}$. Then, every element in $\mathbb{F}_p^*$ is represented by

$$g^{ik+j}, \text{ where } 0 \leq i \leq (p-1)/k - 1,\ 0 \leq j \leq k-1. \quad (3)$$

Therefore, since $\left(g^{ik+j}/p\right)_k$ is evaluated as ϵ_k^j, the number of elements such that its k-th power residue symbol becomes ϵ_k^j is equal to $(p-1)/k$. The others are k-th PNRs. □

2.3 Trace and Its Properties

This paper uses the trace function to map an extension field element $X \in \mathbb{F}_{p^m}$ to a prime field element $x \in \mathbb{F}_p$ as

$$x = \mathrm{Tr}(X) = \sum_{i=0}^{m-1} X^{p^i}. \quad (4)$$

The trace function has a linearity property over the prime field $\mathbb{F}_p$ as follows, where $a, b \in \mathbb{F}_p$ and $Y \in \mathbb{F}_q$.

$$\mathrm{Tr}(aX + bY) = a\mathrm{Tr}(X) + b\mathrm{Tr}(Y). \quad (5)$$

[†]It consists of values from 0 to $p-1$ as elements in $\mathbb{F}_p$.

The following property of the trace function will be useful:

Property 3. *For each $i = 0, 1, 2, \cdots, p-1 \in \mathbb{F}_p$, the number of elements in $\mathbb{F}_q$ whose trace with respect to $\mathbb{F}_p$ equals to i is given by $q/p = p^{m-1}$.* □

Thus, the number of elements in $\mathbb{F}_q^*$ whose trace is equal to zero is given by $q/p - 1$.

2.4 Dual Bases

The dual basis used for some proofs in this paper is defined as follows:

Definition 1. *Let $\mathcal{A} = \{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\}$ be a basis in $\mathbb{F}_{p^m}$. The basis $\mathcal{B} = \{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$, such that*

$$\mathrm{Tr}\left(\alpha_i \beta_j\right) = \begin{cases} 1 & \text{when } i = j \\ 0 & \text{when } i \neq j, \end{cases} \tag{6}$$

is called the dual basis of $\mathcal{A}$. □

The dual basis of an arbitrary basis is uniquely determined in [8]. In this paper, the following property [3] is important.

Property 4. *Let $\mathcal{A}$ and $\mathcal{B}$ be a basis and its dual basis in $\mathbb{F}_{p^m}$, respectively. According to the definition of dual basis and the linearity of trace function, if α_l of a basis $\mathcal{A}$ in $\mathbb{F}_{p^m}$ is a non-zero prime field element,*

$$\mathrm{Tr}\left(\alpha_l \beta_j\right) = \alpha_l \mathrm{Tr}\left(\beta_j\right) = \begin{cases} 1 & \text{when } j = l \\ 0 & \text{when } j \neq l \end{cases}, \tag{7}$$

where $0 \leq j \leq m-1$. Thus, when $\alpha_l = 1$, $\mathrm{Tr}(\beta_l) = 1$. □

2.5 Multi-Valued Sequence and Its Periodic Autocorrelation

In this paper, a k-valued sequence S is denoted as:

$$\mathcal{S} = \{s_i\},\ i = 0, 1, 2, \cdots, n-1, \cdots, \tag{8}$$

where $s_i \in \{0, 1, \cdots, k-1\}$ and n is the period of the sequence such as $s_i = s_{n+i}$. The periodic autocorrelation $\mathrm{R}_{\mathcal{S}}(x)$ of sequence $\mathcal{S}$ shifted by x is defined as

$$\mathrm{R}_{\mathcal{S}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{s_{i+x} - s_i}, \tag{9}$$

where $\tilde{\epsilon}_k$ is a primitive k-th root of unity over the *complex numbers*. It follows that

$$\mathrm{R}_{\mathcal{S}}(0) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^0 = n. \tag{10}$$

In the case of $k = 2$, we have that $\tilde{\epsilon}_k = -1$ and $\mathcal{S}$ becomes a binary sequence [3]. According to previous works on geometric sequences [4], [9], [10], a binary sequence is generated with a primitive element ω, trace function $\mathrm{Tr}(\cdot)$, and some binarizing function $f(\cdot)$ as Eq. (11), where the trace function maps an extension field element to a prime field element:

$$\mathcal{S} = \left\{ s_i \mid s_i = f\left(\mathrm{Tr}\left(\omega^i\right)\right) \right\}. \tag{11}$$

As shown below, this paper utilizes the power residue symbol for the above function $f(\cdot)$ by which trace values $\mathrm{Tr}\left(\alpha^i\right)$ are translated to k-values denoted by s_i.

2.6 Linear Complexity

Since this paper considers multi-valued sequences with coefficients $\{0, 1, \cdots, k-1\}$, the linear complexity $\mathrm{LC}(\mathcal{S})$ of sequence $\mathcal{S}$ of period n is defined as follows:

$$\mathrm{LC}(\mathcal{S}) = n - \deg\left(\gcd\left(x^n - 1, h_{\mathcal{S}}(x)\right)\right), \tag{12}$$

where $h_{\mathcal{S}}(x)$ of $\mathcal{S} = \{s_i\}$ is defined as

$$h_{\mathcal{S}}(x) = \sum_{i=0}^{n-1} s_i x^i. \tag{13}$$

It is noted that $\gcd(x^n - 1, h_{\mathcal{S}}(x))$ in Eq. (12) needs to be evaluated over $\mathbb{F}_k$, where k is a prime number such that k divides $p-1$. It is said that the linear complexity of pseudo random sequences for security applications is preferred to be large. On the other hand, as an counter example, it is known that the maximum length sequence of period $p^m - 1$ has the minimal linear complexity m.

3. Proposal of a Multi-Valued Sequence

Let ω and n be a primitive element in extension field $\mathbb{F}_{p^m}$ and the period of the proposed multi-valued sequence, respectively. This paper proposes the following sequence $\mathcal{T}$ by utilizing the trace function, power residue symbol defined by Eq. (2), and a mapping function $f_k(\cdot)$.

$$\mathcal{T} = \{t_i\},\ t_i = f_k\left(\left(\mathrm{Tr}\left(\omega^i\right)/p\right)_k\right), \tag{14a}$$

where $i = 0, 1, 2, \cdots$. We define the mapping function $f_k(\cdot)$, with a k-th primitive root of unity denoted by $\epsilon_k \in \mathbb{F}_p^*$, as follows:

$$f_k(x) = l = \begin{cases} j \bmod k & \text{when } x = \epsilon_k^j, \\ 0 & \text{otherwise, } i.e.\ x = 0. \end{cases} \tag{14b}$$

The number of l's in the proposed multi-valued sequence $\mathcal{T}$ within the period n is shown in Appendix. Since the input for $f_k(x)$ is 0 or ϵ_k^i from Eq. (14a), note that $f_k(x)$ outputs 0 for both cases of $x = 0$ and $1 = \epsilon_k^0$. Thus the period n of the proposed sequence $\mathcal{T}$ is given by:

$$n = \frac{k(p^m - 1)}{p - 1}. \tag{14c}$$

The periodic autocorrelation of $\mathcal{T}$ is given as follows:

Property 5.

$$R_{\mathcal{T}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{t_{i+x}-t_i} = \begin{cases} \dfrac{k(p^m-1)}{p-1} & \text{if } x = 0, \\ \dfrac{k(p^{m-1}-1)}{p-1} + kp^{m-1}\tilde{\epsilon}_k^r & \text{else if } x \text{ is divisible by } n/k, \\ \dfrac{k(p^{m-2}-1)}{p-1} & \text{otherwise.} \end{cases} \quad (15)$$

□

Note that k divides n as shown in Eq. (14c). The periodic autocorrelation of the sequence $\mathcal{T}$ is obtained by combining the following four relations, where $\hat{n} = (p^m-1)/n = (p-1)/k$ and $j = 0, 1, 2, \cdots$. In addition, for the case that x is divisible by n/k, we define $r = (xk/n) \bmod k$.

$$t_{jn+i} = t_i. \quad (16a)$$

$$t_{(kj+r)n/k+i} = \begin{cases} t_i & \text{if } \mathrm{Tr}\left(\omega^i\right) = 0, \\ r + t_i \bmod k & \text{otherwise.} \end{cases} \quad (16b)$$

$$\sum_{i=0}^{p^m-2} \tilde{\epsilon}_k^{t_{i+x}-t_i} = \hat{n}\mathrm{R}_{\mathcal{T}}(x). \quad (16c)$$

$$\sum_{i=0}^{p^m-2} \tilde{\epsilon}_k^{t_{i+x}-t_i} = \begin{cases} p^{m-1} - 1 + (p^m - p^{m-1})\tilde{\epsilon}_k^r & \text{if } n/k \text{ divides } x, \\ p^{m-2} - 1 & \text{otherwise.} \end{cases} \quad (16d)$$

According to Prop. 1, let $\omega^{n/k} = \omega^{(p^m-1)/(p-1)}$ be a generator g of $\mathbb{F}_p^*$. Then $\omega^n = g^k$ is a k-th power residue in $\mathbb{F}_p^*$.

In addition, for simplicity of discussion, let $\left(g/p\right)_k$ be ϵ_k in what follows. According to the definition of the mapping function $f_k(\cdot)$, t_i shown in Eq. (14a) satisfies

$$\left(\mathrm{Tr}\left(\omega^i\right)/p\right)_k = \epsilon_k^{t_i}. \quad (17)$$

3.1 Overview of the Proof of Prop. 5

In Eq. (15), if $x = 0$, we have

$$\mathrm{R}_{\mathcal{T}}(x) = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^{t_i-t_i} = \sum_{i=0}^{n-1} \tilde{\epsilon}_k^0 = \frac{k(p^m-1)}{p-1}. \quad (18)$$

Otherwise, dividing Eqs. (16c) and (16d) by $\hat{n} = (p-1)/k$, Prop. 5 is proven. In what follows, Eqs. (16c) and (16d) are proven with Eq. (16a) and Eq. (16b), respectively.

3.2 Proof of Eq. (16a)

First, the linearity of trace function leads to

$$t_{jn+i} = f_k\left(\left(\mathrm{Tr}\left(\omega^{jn+i}\right)/p\right)_k\right) = f_k\left(\left(g^{kj}\mathrm{Tr}\left(\omega^i\right)/p\right)_k\right). \quad (19)$$

Then, corresponding to whether or not $\mathrm{Tr}\left(\omega^i\right) = 0$, the power residue symbol leads to

$$t_{jn+i} = \begin{cases} f_k\left(\left(\mathrm{Tr}\left(\omega^i\right)/p\right)_k\right) = 0 = t_i & \text{if } \mathrm{Tr}\left(\omega^i\right) = 0, \\ f_k\left(\left(g^{kj}/p\right)_k\left(\mathrm{Tr}\left(\omega^i\right)/p\right)_k\right) = t_i & \text{otherwise.} \end{cases} \quad (20)$$

Thus, it is shown that t_{jn+i} is equal to t_i regardless of whether or not $\mathrm{Tr}\left(\omega^i\right) = 0$.

3.3 Proof of Eq. (16b)

Similar to Sect. 3.2, we have that

$$t_{(kj+r)n/k+i} = f_k\left(\left(g^{kj+r}\mathrm{Tr}\left(\omega^i\right)/p\right)_k\right). \quad (21)$$

Then, corresponding to whether or not $\mathrm{Tr}\left(\omega^i\right) = 0$,

$$t_{(kj+r)n/k+i} = \begin{cases} f_k\left(\left(\mathrm{Tr}\left(\omega^i\right)/p\right)_k\right) = 0 = t_i & \text{if } \mathrm{Tr}\left(\omega^i\right) = 0, \\ f_k\left(\left(g^r/p\right)_k\left(\mathrm{Tr}\left(\omega^i\right)/p\right)_k\right) = r + t_1 \bmod k & \\ \text{otherwise.} & \end{cases} \quad (22)$$

3.4 Proof of Eq. (16c)

According to Eq. (16a), the left hand side of Eq. (16c) becomes

$$\begin{aligned} \sum_{i=0}^{p^m-2} \tilde{\epsilon}_k^{t_{i+x}-t_i} &= \sum_{j=0}^{\hat{n}-1}\sum_{i=0}^{n-1} \tilde{\epsilon}_k^{t_{(jn+i)+x}-t_{(jn+i)}} \\ &= \sum_{j=0}^{\hat{n}-1}\sum_{i=0}^{n-1} \tilde{\epsilon}_k^{t_{i+x}-t_i} \\ &= \sum_{j=0}^{\hat{n}-1} \mathrm{R}_{\mathcal{T}}(x) = \hat{n}\mathrm{R}_{\mathcal{T}}(x). \end{aligned} \quad (23)$$

3.5 Proof of Eq. (16d)

Consider the following two cases.

3.5.1 If n/k Divides x

According to Eq. (16b), t_{i+x} becomes t_i or $r + t_i \bmod k$ corresponding to $\mathrm{Tr}\left(\omega^i\right) = 0$ or not. Let the number of ω^i's for $i = 0, 1, 2, \cdots, p^m - 2$ such that $\mathrm{Tr}\left(\omega^i\right) = 0$ be $N_{\mathrm{Tr}(\omega^i)=0}$. Then, the following relation is obtained.

$$\sum_{i=0}^{p^m-2} \tilde{\epsilon}_k^{t_{i+x}-t_i} = N_{\mathrm{Tr}(\omega^i)=0} + \left(p^m - 1 - N_{\mathrm{Tr}(\omega^i)=0}\right)\tilde{\epsilon}_k^r. \quad (24)$$

Since the number of trace zero elements including the zero vector is p^{m-1}, $N_{\mathrm{Tr}(\omega^i)=0}$ is given by:

$$N_{\mathrm{Tr}(\omega^i)=0} = p^{m-1} - 1. \quad (25)$$

Thus, the following relation is obtained.

$$\sum_{i=0}^{p^m-2} \tilde{\epsilon}_k^{t_{i+x}-t_i} = p^{m-1} - 1 + (p^m - p^{m-1})\tilde{\epsilon}_k^r. \quad (26)$$

3.5.2 Otherwise

In this case, ω^x does not belong to $\mathbb{F}_p$. Let the basis for representing elements in $\mathbb{F}_{p^m}$ be

$$\{\omega^x, 1, \alpha_2, \alpha_3, \cdots, \alpha_{m-1}\} \quad (27)$$

in which $\alpha_2, \alpha_3, \cdots, \alpha_{m-1}$ can be arbitrary linearly independent elements. It is important that the above basis includes $\omega^x \notin \mathbb{F}_p$ and $1 \in \mathbb{F}_p$. Suppose its dual basis is:

$$\{\beta_0, \beta_1, \beta_2, \beta_3, \cdots, \beta_{m-1}\}. \quad (28)$$

An arbitrary element in $\mathbb{F}^*_{p^m}$ is uniquely represented with this dual basis as:

$$\omega^i = \sum_{k=0}^{m-1} c_{i,k}\beta_k, \ c_{i,k} \in \mathbb{F}_p. \quad (29)$$

According to Prop. 4, its trace is given by:

$$\mathrm{Tr}\left(\omega^i\right) = \sum_{k=0}^{m-1} c_{i,k}\mathrm{Tr}\left(\beta_k\right) = c_{i,1}. \quad (30)$$

On the other hand, the trace of ω^{i+x} is given by

$$\mathrm{Tr}\left(\omega^{i+x}\right) = \mathrm{Tr}\left(\omega^i \cdot \omega^x\right) = \sum_{k=0}^{m-1} c_{i,k}\mathrm{Tr}\left(\beta_k\omega^x\right) = c_{i,0}. \quad (31)$$

Thus, $t_{i+x} - t_i$ is represented as:

$$t_{i+x} - t_i = f_k\left(\left(c_{i,0}/p\right)_k\right) - f_k\left(\left(c_{i,1}/p\right)_k\right). \quad (32)$$

Since ω^i represents every non-zero element in $\mathbb{F}_{p^m}$ with $i = 0, 1, 2, \cdots, p^m - 2$, the relation shown in Eqs. (33) below is obtained to which Prop. 2 needs to be referred. The second term of the right hand side of Eq. (33a) below is for excluding the zero vector.

3.6 Small Examples

Then, the proposed binary sequence of period $n = 8$ given by Eqs. (14) is obtained as follows.

Example 1

Let $p = 11$, $m = 2$, and $k = 2$. Let the primitive polynomial $f(x)$ be $x^2 + 3x + 6$ and its zero be ω in $\mathbb{F}_{11^2}$. Then a binary sequence of period $n = 24$ is obtained as

$$\mathcal{T} = \{1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0\}. \quad (34)$$

Its autocorrelation is given as follows. For simplicity, they are given as absolute values followed by the ceil function.

$$\lceil |\mathrm{R}_{\mathcal{T}}(i)| \rceil = \begin{cases} 24 & \text{when } i = 0 \\ 20 & \text{when } i = 12 \\ 0 & \text{otherwise} \end{cases}. \quad (35)$$

Example 2

Let $p = 7$, $m = 3$, and $k = 3$. Let the primitive polynomial $f(x)$ be $x^3 + 2x^2 + 6x + 2$ and its zero be ω in $\mathbb{F}_{7^3}$. Then, the proposed binary sequence of period $n = 171$ is obtained as

$$\mathcal{T} = \{1, 2, 0, 0, 0, 0, 1, 2, 0, 0, 2, \cdots \cdots, 2, 0, 2, 0, 1, 0, 1, 0, 1, 1, 2, 0, 1\}. \quad (36)$$

In the same way as Eq. (35), its autocorrelation becomes

$$\lceil |\mathrm{R}_{\mathcal{T}}(i)| \rceil = \begin{cases} 171 & \text{when } i = 0 \\ 137 & \text{when } i = 57,\ 114 \\ 3 & \text{otherwise} \end{cases}. \quad (37)$$

4. Linear Complexity

The linear complexity of the proposed sequences was computed for many values of p, m, and k. According to the experimental result, $\mathrm{LC}(\mathcal{T})$ was equal to $2(p^m - 1)/(p - 1)$ without any exceptions. It does not depend on k. If this experimental observation is theoretically proven, when $k = 2$ for example, the linear complexity takes the maximum value because the period and the linear complexity are both given by $2(p^m - 1)/(p - 1)$. Its theoretic proof seems to be difficult; however, for $m = 2$, it is proven below.

Let us consider $m = 2$ in what follows. Note that the sequence $\mathcal{T}$ defined by Eq. (14a) consists of $\{0, 1, \cdots, k-1\}$, where k is a prime number that divides $p - 1$ in this paper. Then, consider the following polynomial over $\mathbb{F}_k$ with the proposed multi-valued sequence $\mathcal{T} = \{t_i\}$ of period n.

$$h_{\mathcal{T}}(x) = \sum_{i=0}^{n-1} t_i x^i. \quad (38)$$

Since n is given by $k(p + 1)$ when $m = 2$, it results in Eq. (39a) below, where it should be noted that the trace function has a linearity over $\mathbb{F}_p$ and $\omega^{p+1} \in \mathbb{F}_p$. Since ω is a generator of $\mathbb{F}^*_{p^2}$, ω^{p+1} becomes a generator of $\mathbb{F}^*_p$.

Let $n' = n/k$, that is $n' = (p + 1)$. According to finite field theory [8], among ω^i for $0 \le i < n'$, there is only one element whose trace with respect to $\mathbb{F}_p$ becomes 0. Let the exponent of the element be u. In other words, u satisfies $\mathrm{Tr}(\omega^u) = 0$ and $0 \le u < n'$ and its Legendre symbol

$$\sum_{i=0}^{p^m-2} \tilde{\epsilon}_k^{t_{i+x}-t_i} = p^{m-2} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \tilde{\epsilon}_k^{f_k((u/p)_k)-f_k((v/p)_k)} - \tilde{\epsilon}_k^{f_k((0/p)_k)-f_k((0/p)_k)} \tag{33a}$$

$$= p^{m-2} \sum_{u=0}^{p-1} \tilde{\epsilon}_k^{f_k((u/p)_k)} \sum_{v=0}^{p-1} \tilde{\epsilon}_k^{-f_k((v/p)_k)} - 1 = p^{m-2} \sum_{u=0}^{p-1} \tilde{\epsilon}_k^{f_k((u/p)_k)} - 1 = p^{m-2} - 1. \tag{33b}$$

$$\begin{aligned} h_{\mathcal{T}}(x) = \sum_{i=0}^{k(p+1)-1} t_i x^i &= \sum_{i=0}^{k-1} \left(\sum_{j=0}^{p} f_k \left(\left(\mathrm{Tr}\left(\omega^{i(p+1)+j}\right)/p \right)_k \right) x^{i(p+1)+j} \right) \\ &= \sum_{i=0}^{k-1} \left(\sum_{j=0}^{p} f_k \left(\left(\omega^{i(p+1)} \mathrm{Tr}\left(\omega^{j}\right)/p \right)_k \right) x^{i(p+1)+j} \right) \\ &= \sum_{i=0}^{k-1} \left(\sum_{j=0}^{p} f_k \left(\epsilon_k^i \left(\mathrm{Tr}\left(\omega^{j}\right)/p \right)_k \right) x^{i(p+1)+j} \right) \qquad (39a) \\ &= \sum_{i=0}^{k-1} \left(\sum_{j=0}^{p} \left((i+t_j) \bmod k \right) x^{i(p+1)+j} - i x^{i(p+1)+u} \right) \\ &= \sum_{i=0}^{k-1} \left(\sum_{j=0}^{p} \left(i x^{i(p+1)+j} + t_j x^{i(p+1)+j} \right) - i x^{i(p+1)+u} \right) \\ &= \sum_{i=0}^{k-1} x^{i(p+1)} \left(\sum_{j=0}^{p} \left(t_j x^j \right) \right) + \sum_{i=0}^{k-1} i x^{i(p+1)} \left(\sum_{j=0}^{p} x^j - x^u \right) \\ &\equiv \left(x^{p+1} - 1 \right)^{k-1} \left(\sum_{j=0}^{p} \left(t_j x^j \right) \right) + \left(x^{p+1} - 1 \right)^{k-2} \left(\sum_{j=0}^{p} x^j - x^u \right) \pmod{k} \\ &\equiv \left(x^{p+1} - 1 \right)^{k-2} \left(\left(x^{p+1} - 1 \right) \left(\sum_{j=0}^{p} \left(t_j x^j \right) \right) + \frac{\left(x^{p+1} - 1 \right)}{x - 1} - x^u \right) \pmod{k}. \qquad (39b) \end{aligned}$$

$\left(\mathrm{Tr}\left(\omega^u\right)/p\right)_k$ is equal to 0. Therefore, let $\left(\omega^{p+1}/p\right)_k = \epsilon_k \in \mathbb{F}_p^*$, for $0 \le i \ne u < n'$. Then the following relation holds:

$$\begin{aligned} f_k \left(\left(\omega^{i(p+1)} \mathrm{Tr}\left(\omega^j\right)/p \right)_k \right) &= f_k \left(\epsilon_k^i \left(\mathrm{Tr}\left(\omega^j\right)/p \right)_k \right) \\ &= f_k \left(\epsilon_k^i \epsilon_k^{t_j} \right) = i + t_j. \end{aligned} \tag{40a}$$

For $i = u$, according to $\left(0/p\right)_k = 0$ and Eq. (14b),

$$f_k \left(\left(\omega^{i(p+1)} \mathrm{Tr}\left(\omega^u\right)/p \right)_k \right) = f_k(0) = 0. \tag{40b}$$

Substituting these relations to Eq. (39a) with respect to u, Eq. (39b) is obtained. Thus, for $m = 2$, $\mathrm{LC}(\mathcal{T})$ for the proposed multi-valued sequence $\mathcal{T}$ is given by

$$\begin{aligned} \mathrm{LC}(\mathcal{T}) &= n - \deg\left(\gcd\left(x^n - 1, h_{\mathcal{T}}(x)\right)\right) \\ &= k(p+1) - \deg\left(\gcd\left((x^{(p+1)} - 1)^k, h_{\mathcal{T}}(x)\right)\right) \\ &= k(p+1) - (k-2)(p+1) \\ &= 2(p+1). \end{aligned} \tag{41}$$

In the calculations of Eqs. (39) and Eq. (41), it should carefully noted that polynomials are defined over $\mathbb{F}_k$. In addition, note that $(x^{p+1}-1)/(x-1) - x^u$ in Eq. (39b) is not divisible by $x-1$ over $\mathbb{F}_k$ since k is a prime factor of $p-1$ in this paper. As shown above, in the case of $m = 2$, it has been theoretically proven that the proposed sequence has the linear complexity $2n/k$, or $2(p^m - 1)/(p - 1)$. This does not depend on the parameter k. For the other cases, as previously indicated, such a typical feature has been experimentally observed.

4.1 Small Examples

Example 1

For the sequence Eq. (34), where $p = 11$, $m = 2$, and $k = 2$, the linear complexity becomes maximum and equal to 24. This was shown as the preceding theoretic proof.

Example 2

For the sequence Eq. (36), where $p = 7$, $m = 3$, and $k = 2$, the linear complexity becomes 114. This was experimentally observed.

5. Conclusion and Future Works

In this paper, a method was proposed to generate multi-valued sequences including binary sequences based on a primitive element over odd characteristic field $\mathbb{F}_{p^m}$, the trace function and power residue symbols. Some typical features were analyzed, such as period, periodic autocorrelation and its maximal and minimal values, the number of values in the sequence per period, and the linear complexity. Specifically for the case of $m = 2$, the linear complexity was theoretically shown. Some experimental observations were also introduced. As future works, the following points should be researched:

- Cross-correlations with other primitive polynomials.
- Other tools instead of power residue symbol.
- Observing the distribution of bit patterns.
- Evaluating the randomness.
- Efficient algorithm to generate the proposed sequence.

Acknowledgment

This research was supported in part by KAKENHI Grant-in-Aid for Scientific Research (B) Number 25280047.

References

[1] S.W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, 1967.
[2] N. Zierler, Legendre Sequence, M.I.T. Lincoln Publications, 1958.
[3] Y. Nogami, K. Tada, and S. Uehara, "A geometric sequence binarized with legendre symbol over odd characteristic field and its properties," IEICE Trans. Fundamentals, vol.E97-A, no.12, pp.2336–2342, Dec. 2014.
[4] A.H. Chan and R. Games, "On the linear span of binary sequences from finite geometries, q odd," IEEE Trans. Inf. Theory, vol.36, no.3, pp.548–552, 1990.
[5] W. Sun, A. Klapper, and Y.X. Yang, "On correlations of a family of generalized geometric sequences," IEEE Trans. Inf. Theory, vol.47, no.6, pp.100–109, 2001.
[6] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation," IEEE Trans. Inf. Theory, vol.48, no.11, pp.2868–2872, 2002.
[7] G. Gong and H.Y. Song, "Two-tuple balance of non-binary sequences with ideal two-level autocorrelation," Discrete Appl. Math., vol.154, no.18, pp.2590–2598, Elsevier, 2006.
[8] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1984.
[9] A. Klapper, "Cross-correlations of geometric sequences in characteristic two," Des. Codes Crypt., vol.3, no.4, pp.347–377, 1993.
[10] A. Klapper, "Large families of sequences with low correlations and large linear span," IEEE Trans. Inf. Theory, vol.42, no.4, pp.1241–1248, 1996.

Appendix: The number of l's in $\mathcal{T}$

Denote the number of l's, $l \in \mathbb{F}_k$ in the proposed sequence $\mathcal{T} = \{t_i\}$ within a period by $N_{t_i=l}$. Then, they are given by

$$N_{t_i=0} = p^{m-1} + \frac{k(p^{m-1}-1)}{p-1}, \tag{A· 1a}$$

$$N_{t_i=l,\ l\neq 0} = p^{m-1}. \tag{A· 1b}$$

As shown above, the number of 0's are relatively larger than those of the others. It is caused by the mapping function $f_k(\cdot)$ defined by Eq. (14b). When $m = 2$, the difference between $N_{t_i=0}$ and $N_{t_i=l,\ l\neq 0}$ is just k. Of course, $\sum_{0\le l<k} N_{t_i=l}$ is just n that is the period of the sequence. It is proven as follows.

Let $n' = n/k = (p^m-1)/(p-1)$ and let ω be a primitive element in $\mathbb{F}^*_{p^m}$. Since the period of the proposed sequence $\mathcal{T}$ is equal to n, let us consider n non-zero elements in $\mathbb{F}^*_{p^m}$ as ω^i for $i = 0, 1, 2, \cdots, n-1$. Note that $\omega^{n'} = \omega^{(p^m-1)/(p-1)} = g$ becomes a generator of $\mathbb{F}^*_p$. According to Eq. (16b), the following relation holds for $0 \le u < k$ and $0 \le v < n'$.

$$f_k\left(\left(\mathrm{Tr}\left(\omega^{un'+v}\right)/p\right)_k\right) = \begin{cases} 0 & \text{when } \mathrm{Tr}\left(\omega^v\right) = 0 \\ u + t_v \bmod k & \text{otherwise} \end{cases}. \tag{A· 2}$$

Here note that $N_{t_i=0}$ is given by the sum of the following numbers N_1 and N_2 for $0 \le i < n$, $0 \le u < k$, and $0 \le v < n'$. N_1 is the number of cases such that

$$\mathrm{Tr}\left(\omega^i\right) = 0. \tag{A· 3a}$$

N_2 is the number of cases such that

$$u + t_v = 0 \text{ and } \mathrm{Tr}\left(\omega^{un'+v}\right) \neq 0. \tag{A· 3b}$$

Then, the former N_1 is given by

$$N_1 = \frac{k(p^{m-1}-1)}{(p-1)}. \tag{A· 4}$$

On the other hand, the latter N_2 is given by[†]

$$N_2 = (n - N_1)/k = p^{m-1}. \tag{A· 5}$$

Finally, Eqs. (A· 1) are obtained.

[†]It is because, for $0 \le l < k$, the number of cases such that $u + t_v = l$ and $\mathrm{Tr}\left(\omega^{un'+v}\right) \neq 0$ becomes the same.

Begum Nasima received her Ph.D. in Cryptography and Information Security from Okayama University, Japan in 2014. She received the B.Sc. and M.Sc. in Computer Science and Engineering from Jahangirnagar University, Bangladesh in 2006 and 2010 respectively. She joined as a Lecturer at the department of Computer Science and Engineering, Manarat International University, Bangladesh in January 2007. Currently, she is working as an Assistant Professor at the department of Computer Science and Engineering, University of Asia Pasific, Bangladesh. She has worked as a Foreign Research Fellow in Secure Wireless System Lab, Okayama University, Japan, from October 2014 to March 2016. Her research interest includes cryptography and information security, signal and image processing, and artificial intelligence. She is a member of IEEE, ACM and IEICE.

Yasuyuki Nogami graduated from Shinshu University in 1994 and received the Ph.D. degree in 1999 from Shinshu University. He is now an associate professor of Okayama University. His main fields of research are finite field theory and its applications such as recent public key cryptographies. He is now studying about elliptic curve cryptography, pairing-based cryptography, Lattice-based cryptography, pseudo random number generator, Advanced Encryption Standard, and homomorphic encryptions. Recently, he is a member of security research group in Okayama university and particularly focusing on IoT security from the viewpoints of software and hardware implementations. He is a member of IEICE and IEEE.

Satoshi Uehara received the B.E. degree from Saga University and the M.E. degree from Kyushu University, and the Dr. Eng. degree in computer science and system engineering from Kyushu Institute of Technology, in 1987, 1989 and 1998, respectively. From 1989 to 2000, he was a research associate at Kyushu Institute of Technology. From 2000, he was with the Department of Information and Media Engineering, The University of Kitakyushu as associate professor, and became a professor in 2009. He is engaged in research on sequence design for cryptography and spread spectrum applications.

Robert H. Moleros-Zaragoza received the BSEE and MSEE degrees from the National Autonomous University of Mexico (UNAM) in 1985 and 1987, respectively, and the Ph.D. degree in Electrical Engineering from the University of Hawaii at Manoa in 1992. Robert has research interests in the areas of error correcting coding and digital signal processing for wireless communication and digital storage systems. He is the author of twenty peer-reviewed journal papers, over ninety international peer-reviewed conference papers and the book The Art of Error Correcting Coding (2nd edition, John Wiley and Sons, 2006). Prof. Morelos-Zaragoza holds eighteen patents in the USA, Japan and Europe, and has served as reviewer, editor and technical program committee member in numerous international IEEE conferences and journals in Information Theory and Wireless Communication Systems.