Periodic Autocorrelation of A Signed Binary Sequence Additively Generated With Trace Over Odd Characteristic Extension Field

Yasuyuki Nogami[1] and Satoshi Uehara[2]
[1]Graduate School of Natural Science and Technology, Okayama University,
3-1-1, Tsushima-naka, Kita, Okayama, 700-8530,
E-mail: yasuyuki.nogami@okayama-u.ac.jp.
[2]Graduate School of Environmental Engineering,
The University of Kitakyushu, 1-1 Hibikino, Wakamatsu, Kitakyushu, Fukuoka, 808-0135,
E-mail: uehara@kitakyu-u.ac.jp.

Abstract: Pseudo random binary sequence has been well studied such as maximal length sequence and Legendre sequence. Combining their generation approaches such as trace function and Legendre symbol, a binary sequence was proposed and its features such as period and autocorrelation were also discussed. These sequences have use a primitive element in order to systematically generate a maximum length vector sequence. Instead of this *multiplicative* procedure with a primitive element, this paper applies an *additive* procedure with focusing on the basis of the extension field. Then, it is experimentally observed that, when the basis is Gauss period normal basis, the autocorrelation graph has a typical feature.

1. Introduction

Pseudo random sequence plays an important role in the recent cryptographic protocols. Maximal length sequence (M-sequence) [1] and Legendre sequence [2] have been well known because their features such as period, periodic autocorrelation, and linear complexity are theoretically given. However, from security viewpoints, they also have some negative points. As an example, the linear complexity of M-sequence is the minimal and there are no varieties of Legendre sequence of the same period. In order to overcome these inefficiency, our previous work has combined them [3]. In detail, the pseudo binary random sequence is generated by using a primitive element in an odd characteristic extension field $\mathbb{F}_{p^m}$, trace function, and Legendre symbol. A primitive element is used for generating M-sequence of vectors, trace function maps the vectors to scalars in the prime field $\mathbb{F}_p$, and finally Legendre symbol binarizes the scalars. It has been theoretically shown that it has several interesting features such as period, periodic autocorrelation, and linear complexity.

This paper introduces a new approach that slightly changes a part of the previous generation procedure. It is noted that the previous sequence uses a generator in $\mathbb{F}^*_{p^m}$. In other words, let g be a generator, the binary sequence of the previous work [3] is generated in the order of g^i, $i = 1, 2, 3, \cdots$. This paper changes this part to an additive procedure in the same of p-adic representation. As an example, when $p = 3$ and $m = 3$, it becomes as follows.

$$(0,0,0),(0,0,1),(0,0,2),(0,1,0),(0,1,1),\cdots,\\ (2,0,0),\cdots,(2,2,1),(2,2,2). \quad (1)$$

Then, trace function and Legendre symbol are applied in the same of the previous work [3]. The new approach is closely related to what kind of basis is used for the vector representation such as Eq. (1). This paper applies two types of basis: one is polynomial basis and the other is optimal normal basis. Then, it is shown that a typical difference is observed on their periodic autocorrelations.

2. Previous work

Let $\mathrm{Tr}(\cdot)$, $\left(a/p\right)$, and ω be the trace function that maps a vector in $\mathbb{F}_{p^m}$ to a scalar in $\mathbb{F}_p$, Legendre symbol that is used for mapping a scalar in $\mathbb{F}_p$ to a signed binary value as $\{0, 1, -1\}$, and a zero of $g(x)$ that becomes a primitive element in $\mathbb{F}_{p^m}$, respectively. Then, using a mapping function $f(\cdot)$, the binary sequence $\mathcal{T}$ is defined as follows.

$$\mathcal{T} = \{t_i\},\ t_i = f\left(\left(\mathrm{Tr}\left(\omega^i\right)/p\right)\right),\ i = 0, 1, 2, \cdots, \quad (2)$$

where $f(\cdot)$ is defined as

$$f(x) = \begin{cases} 0 & \text{if } x = 0, 1, \\ 1 & \text{otherwise.} \end{cases} \quad (3)$$

Trace function is actually defined as follows.

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

x becomes an element in $\mathbb{F}_p$ and the above trace function has a linearity over $\mathbb{F}_p$ as follows, where $a, b \in \mathbb{F}_p$ and $Y \in \mathbb{F}_q$.

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

Then, Legendre symbol is calculated as follows.

$$\begin{aligned} \left(a/p\right) &= a^{(p-1)/2} \bmod p \\ &= \begin{cases} 0 & \text{when } a = 0, \\ 1 & \text{if } a \text{ is a non-zero QR}, \\ p-1 & \text{otherwise, that is } a \text{ is a QNR}, \end{cases} \end{aligned} \quad (6)$$

where QR and QNR are abbreviations of quadratic residue and quadratic non-residue, respectively.

2.1 Features of the binary sequence

According to our previous work [3], firstly the period of $\mathcal{T}$ is given as follows.

$$n = \frac{2(p^m - 1)}{p - 1}. \quad (7)$$

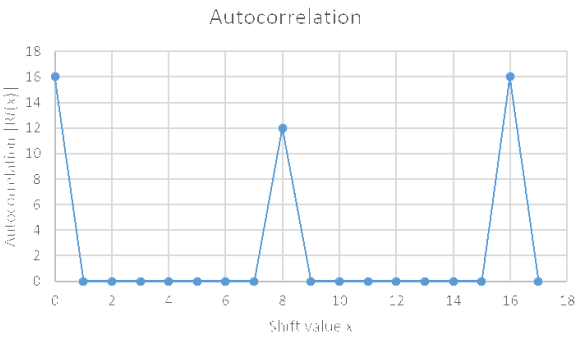

Figure 1. $\bar{\mathrm{R}}_{\mathcal{T}}(x)$ with $p = 7, m = 2$

Let the autocorrelation with shift value x be defined by

$$\bar{\mathrm{R}}_{\mathcal{T}}(x) = \sum_{x=0}^{n-1} (-1)^{t_{i+x} - t_i}, \tag{8}$$

the autocorrelation of $\mathcal{T}$ is given by

$$\bar{\mathrm{R}}_{\mathcal{T}}(x) = \begin{cases} \dfrac{2(p^m - 1)}{p - 1} & \text{if } x = 0, \\ -2p^{m-1} + \dfrac{2(p^{m-1} - 1)}{p - 1} & \text{else if } x = n/2, \\ \dfrac{2(p^{m-2} - 1)}{p - 1} & \text{otherwise.} \end{cases} \tag{9}$$

As a small example, **Figure**. 1 shows the graph of the autocorrelation of $\mathcal{T}$ with $p = 7$ and $m = 2$.

Then, let the definition of linear complexity be

$$\mathrm{LC}(\mathcal{T}) = n - \deg(\gcd(x^n - 1, h_{\mathcal{T}}(x))), \tag{10}$$

where $h_{\mathcal{T}}(x)$ is defined as

$$h_{\mathcal{T}}(x) = \sum_{i=0}^{n-1} t_i x^i. \tag{11}$$

The linear complexity of $\mathcal{T}$ is experimentally observed as

$$\mathrm{LC}(\mathcal{T}) = \frac{2(p^m - 1)}{p - 1}. \tag{12}$$

Particularly when $m = 2$, it has been theoretically proven.

In addition, let N_0 and N_1 be the numbers of 0's and 1's, respectively, they are theoretically proven as

$$N_0 = p^{m-1} + \frac{2(p^{m-1} - 1)}{p - 1}, \tag{13a}$$

$$N_1 = p^{m-1}. \tag{13b}$$

As an important point, when $m = 2$, the difference between N_0 and N_1 becomes just 2. It is an important feature for realizing unpredictable random binary sequences.

3. Additively generated sequence

This paper proposes a signed binary sequence that is generated in the mostly similar way of the previous work. There are two important differences. One is that, the previous work generates the next coefficient *multiplicatively* as ω^i in Eq. (2) with a primitive element ω, on the other hand this paper generates additively as Eq. (1). The other is that, the previous work uses a function $f(\cdot)$ defined by Eq. (3) for mapping a signed binary value of Legendre symbol to a non-signed binary value as {0.1}, on the other hand this paper uses signed binary values without applying the mapping function $f(\cdot)$.

3.1 Additive vector order

This paper adapts the following additive vector order. Let $\{\theta_0, \theta_1, \cdots, \theta_{m-1}\}$ be a basis in $\mathbb{F}_{p^m}$. Then, an arbitrary vector A in $\mathbb{F}_{p^m}$ is represented as follows.

$$A = (a_0, a_1, \cdots, a_{m-1}) = \sum_{j=0}^{m-1} a_j \theta_j, \ a_j \in \mathbb{F}_p. \tag{14}$$

It is obvious that there are p^m vectors as from $(0, 0, \cdots, 0)$ to $(p-1, p-1, \cdots, p-1)$. In the similar way of p-adic representation, define the following notation:

$$\omega_i = (w_0, w_1, \cdots, w_{m-1}) = \sum_{j=0}^{m-1} w_j \theta_j, \ w_j \in \mathbb{F}_p,$$
$$st. \sum_{j=0}^{m-1} w_j p^j = i. \tag{15}$$

Example 1: When $p = 3$ and $m = 3$, there are 27 vectors in $\mathbb{F}_{3^3}$ and this paper denotes them such as

$$\omega_5 = (2, 1, 0), \ \ \omega_{22} = (1, 1, 2). \tag{16}$$

3.2 Definition of the proposed sequence

Based on the above definition of ω_i, this paper proposes the following signed binary sequence $\mathcal{S}$.

$$\mathcal{S} = \{s_i\}, \ s_i = \left(\mathrm{Tr}\left(\omega_i\right)/p\right), \ i = 0, 1, 2, \cdots, p^m - 1 \tag{17}$$

Though there are several viewpoints such as period, periodic autocorrelation, and linear complexity, this paper experimentally observes its periodic autocorrelation. It is easily found that its period n becomes $p^m - 1$.

4. Experiments

This paper experimentally observes the periodic autocorrelation of the proposed signed binary sequence $\mathcal{S}$. There are several types of basis for $\mathbb{F}_{p^m}$ such as polynomial basis, normal basis, Gauss period normal basis. This paper has applied a polynomial basis and Gauss period normal basis. It is noted that Gauss period normal basis has been well studied [4]. Without loss of generality, this paper slightly changes the

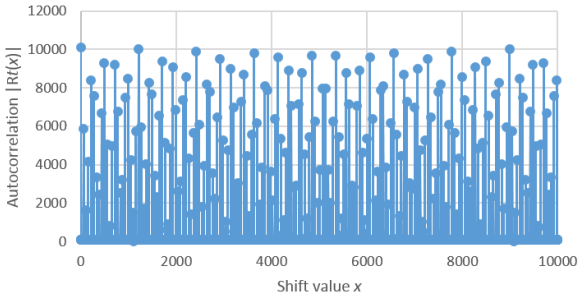

Figure 2. $\bar{\mathrm{R}}_{\mathcal{S}}(x)$ with $p = 101, m = 2$, **(polynomial basis)**

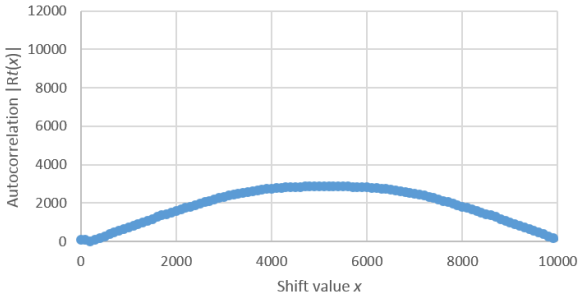

Figure 5. $\bar{\mathrm{R}}_{\mathcal{S}}(x)$ with $p = 101, m = 2$, such that $x \bmod 100 = 1$, **(normal basis)**

evaluation of periodic autocorrelation for the proposed signed binary sequence $\mathcal{S}$ as follows.

$$\mathrm{R}_{\mathcal{S}}(x) = \sum_{x=0}^{n-1} s_{i+x} * s_i, \tag{18}$$

Firstly, **Figure**. 2 shows the autocorrelation graph of the proposed signed binary sequence that uses a polynomial basis representation with $p = 101$ and $m = 2$. It seems to have some periodic features, however it has not been explicitly observed. On the other hand, **Figure**. 3 shows the case of Gauss period normal basis. It is obviously found that it has an typical feature. In order to show the feature more clearly, **Figure**. 4 has picked up the correlation when the shift value x satisfies $x \bmod 101 = 0$, where it is noted that $p = 101$ and $p - 1 = 100$. **Figure**. 5 has picked up the correlation when the shift value x satisfies $x \bmod 101 = 1$

According to these graphs, the periodic autocorrelation of the proposed signed binary sequence $\mathcal{S}$ depends on the choice of basis. Particularly, when Gauss period normal basis is applied, a typical feature has been observed as **Figure**. 3.

5. Conclusion and future works

This paper has proposed a signed binary sequence generated by trace and Legendre symbol for which an additive vector order has been considered. Then, corresponding to the applied basis, this paper experimentally observed the periodic autocorrelation. Particularly when the basis was Gauss period normal basis, the autocorrelation had a typical feature. As future works, its theoretic proof should be considered and then its practical application should be also discussed.

References

[1] S. W. Golomb, "Shift Register Sequences," Holden-Day, San Francisco, 1967.

[2] J. S. No, H. K. Lee, H. Chung, H. Y. Song, and K. Yang, "Trace Representation of Legendre Sequences of Mersenne Prime Period," IEEE Trans. on Inform. Theory, vol. 42, pp. 2254–2255, 1996.

[3] Y. Nogami, K. Tada, and S. Uehara, "A Geometric Sequence Binarized with Legendre Symbol over Odd Characteristic Field and Its Properties," IEICE Trans., vol. 97-A, no. 12, pp. 2336–2342, 2014.

[4] K. Nekado, Y. Nogami, H. Kato, and Y. Morikawa, "Cyclic Vector Multiplication Algorithm and Existence Probability of Gauss Period Normal Basis," IEICE Transactions 94-A(1), pp. 172–179, 2011.

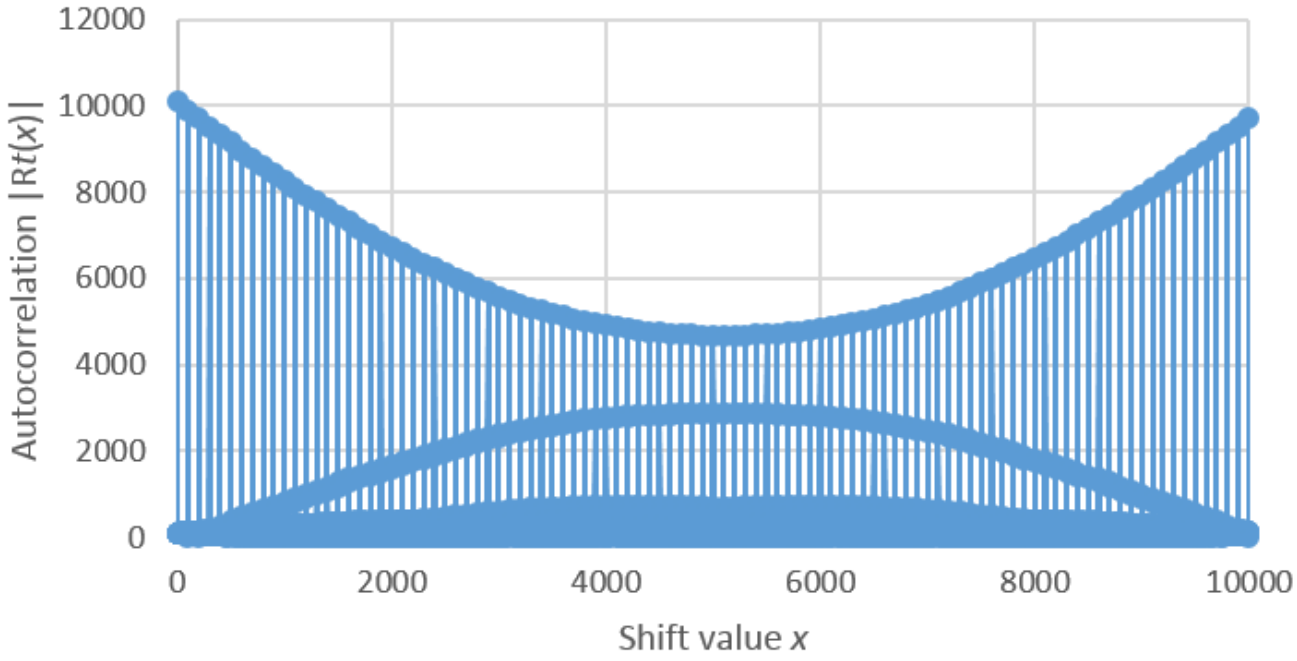

Figure 3. $\bar{\mathrm{R}}_{\mathcal{S}}(x)$ with $p = 101, m = 2$, **(normal basis)**

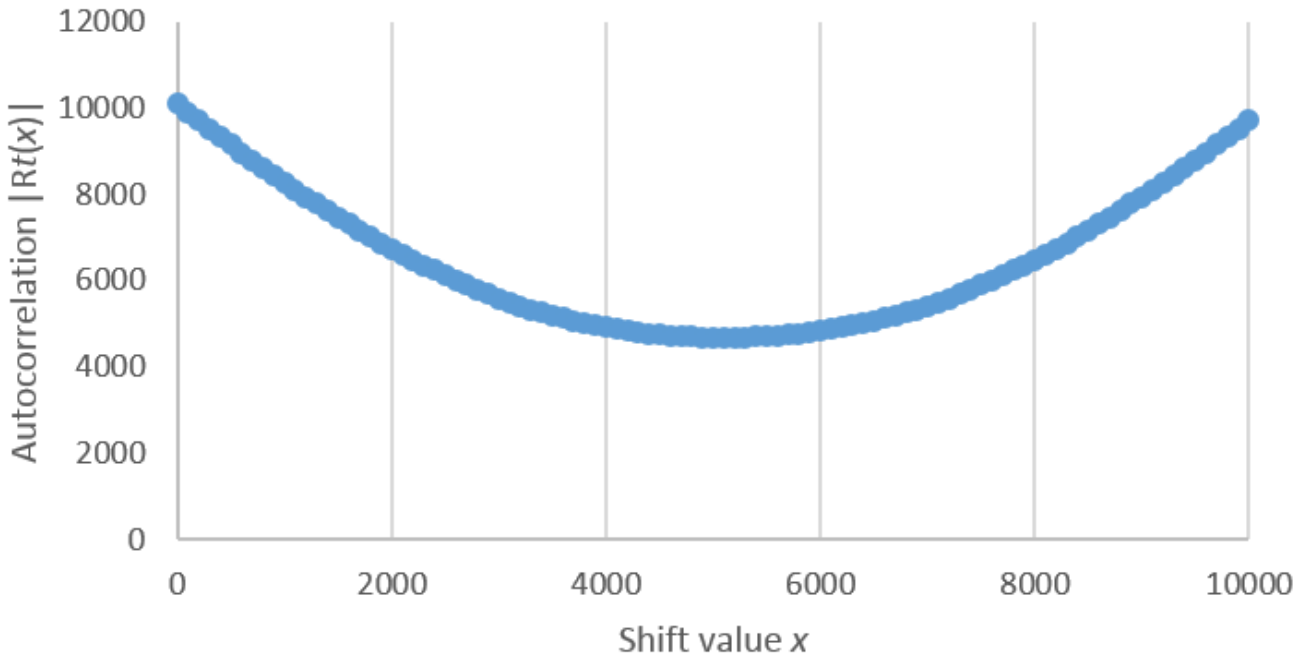

Figure 4. $\bar{\mathrm{R}}_{\mathcal{S}}(x)$ with $p = 101, m = 2$, such that $x \bmod 100 = 0$, **(normal basis)**