2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Pseudo Random Binary Sequence Generated by Trace and Legendre Symbol with Non Primitive Element in $\mathbb{F}_{p^2}$

C. Ogawa†, A. M. Arshad†, Y. Nogami†, S. Uehara‡, K. Tsuchiya††, and R. M. Zaragoza‡‡

† 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.
‡ Graduate School of Environmental Engineering, The University of Kitakyushu,
1-1, Hibikino, Wakamatsu, Kitakyushu, Fukuoka, 808-0135, E-mail: uehara@kitakyu-u.ac.jp.
†† Koden Electronics Co. Ltd., 2-13-24 Tamagawa, Ota-ku, Tokyo, 146-0095,
E-mail:k-tsuchiya@koden-electronics.co.jp.
‡‡ Department of Electrical Engineering San Jose State University,
1 Washington Square, San Jose, CA 95192-0084, E-mail: R.Morelos-Zaragoza@IEEE.org.

Abstract—Pseudo binary random sequence has many uses such as nonce for security applications. Some of them needs to have long period and high linear complexity. The authors have proposed a generation method that uses primitive polynomial, trace function, and Legendre symbol over odd characteristic field. The preparation of primitive polynomial is not always easy. This paper shows that some non-primitive irreducible polynomials generate the same random binary sequence generated by a certain primitive polynomial. Then, some example are also introduced.

1. Introduction

There are many kinds of pseudo binary random sequence generated over finite fields. Among them, maximal length sequence (M-sequence) and Legendre sequence are well known [1],[2]. M-sequence uses trace function and Legendre sequence uses Legendre symbol. Their typical properties such as period, autocorrelation, and linear complexity have been theoretically shown. The authors have proposed a pseudo binary random sequence generated by primitive polynomial, trace function, and Legendre symbol [3]. It has long period and high linear complexity. These properties have been theoretically shown. Different from M-sequence and Legendre sequence, this sequence has two parameters p and m, where p and m are the characteristic and extension degree by which the base extension field $\mathbb{F}_{p^m}$ is defined. In addition, in the same of M-sequence, it also needs a primitive polynomial.

In order to prepare a long period sequence for some cryptographic applications, the characteristic p or the extension degree m should be large. Accordingly, the previous sequence needs to prepare a primitive polynomial of degree m over $\mathbb{F}_p$. However, the preparation is not always easy. This paper shows some non-primitive irreducible polynomials are able to generate the same sequence generated by a certain primitive polynomial. If the condition is clearly given, the preparation of the non-primitive irreducible polynomial will be easier than that of primitive polynomial. When the degree m is restricted to 2, this paper not only considers the conditions but also shows some examples.

2. Preparation

This section briefly introduces some mathematical tools. Throughout this paper, p be an odd prime number.

2.1. Irreducible and primitive polynomials

Let $\mathbb{F}_p$ be a prime field of odd characteristic p. When $f(x)$ of degree m over $\mathbb{F}_p$ is not factorized into smaller degree polynomials over $\mathbb{F}_p$, it is called irreducible polynomial. Let ω be its zero, ω belongs to the extension field $\mathbb{F}_{p^m}$ and its order e is a divisor of p^m-1. It is noted that p^m-1 is the order of the multiplicative group $\mathbb{F}^*_{p^m} = \mathbb{F}_{p^m} - \{0\}$. Particularly when $e = p^m - 1$, it is called a primitive polynomial and its zero is called a primitive element in $\mathbb{F}_{p^m}$ correspondingly. M-sequence and our previous work [3] utilize a primitive element to generate a maximal length sequence because the primitive element ω is able to represent all non-zero elements as its power ω^i, $i = 0, 1, 2, \cdots, p^m-2$. When $m = 2$, an irreducible polynomial of degree 2 over $\mathbb{F}_p$ is easily generated even if p is large.

2.2. Trace function and Legendre symbol

Consider an extension field $\mathbb{F}_{p^m}$. Then, trace function for $X \in \mathbb{F}_{p^m}$ is defined as follows.

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

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

$$\mathrm{Tr}(aX + bY) = a\mathrm{Tr}(X) + b\mathrm{Tr}(Y), \tag{2}$$

where $a, b \in \mathbb{F}_p$ and $Y \in \mathbb{F}_{p^m}$. In the previous work [3], trace function is used for mapping a vector in $\mathbb{F}_{p^m}$ to a scalar in $\mathbb{F}_p$. Then, Legendre symbol is calculated as follows.

$$\begin{aligned} \left(\frac{a}{p}\right) &= a^{(p-1)/2} \bmod p \\ &= \begin{cases} 0 & \text{when } a = 0, \\ 1 & \text{if } a \text{ is a non-zero QR}, \\ -1 & \text{otherwise, that is } a \text{ is a QNR}, \end{cases} \end{aligned} \tag{3}$$

where QR and QNR are abbreviations of quadratic residue and quadratic non-residue, respectively. In our previous work, Legendre symbol is used for mapping a scalar in $\mathbb{F}_p$ to a signed binary value such as $\{0, 1, -1\}$.

2.3. Previous work

The previous work [3] has proposed a pseudo random binary sequence generated by using primitive polynomial, trace function, and Legendre symbol as follows.

$$\mathcal{T} = \{t_i\},\ t_i = f\left(\left(\frac{\mathrm{Tr}\left(\omega^i\right)}{p}\right)\right),\ i = 0, 1, 2, \cdots, \tag{4}$$

where $f(\cdot)$ is defined as

$$f(x) = \begin{cases} 0 & \text{if } x = 0, 1, \\ 1 & \text{otherwise.} \end{cases} \tag{5}$$

ω in Eq. (4) is a primitive element in $\mathbb{F}_{p^m}$. Then, its period is given by $2(p^m - 1)/(p - 1)$.

Let the autocorrelation with shift value x be defined by

$$\mathrm{R}_{\mathcal{T}}(x) = \sum_{x=0}^{n-1} (-1)^{t_{i+x} - t_i}, \tag{6}$$

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

$$\mathrm{R}_{\mathcal{T}}(x) = \begin{cases} \dfrac{2(p^m - 1)}{p - 1} & \text{if } x = 0, \\ -2p^{m-1} + \dfrac{2(p^{m-1} - 1)}{p - 1} & \text{else if } x = n/2, \\ \dfrac{2(p^{m-2} - 1)}{p - 1} & \text{otherwise.} \end{cases} \tag{7}$$

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

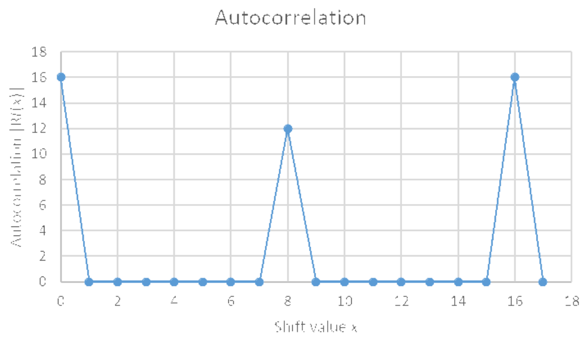

Figure 1: $|\mathrm{R}_{\mathcal{T}}(x)|$ with $p = 7, m = 2$

3. Binary sequence with non-primitive polynomial

This paper introduces, particularly when the extension degree $m = 2$, some non-primitive irreducible polynomials generate the same random binary sequence generated by a certain primitive polynomial.

3.1. Motivation

First of all, when the characteristic p or the degree m are large such as used for cryptographies, preparing a primitive polynomial is not always easy. Let us consider the case that p is a large prime number and $m = 2$. In this case, consider all prime factors p_i of $p^2 - 1$ as

$$p^2 - 1 = \prod_i p_i^{e_i}, \tag{8}$$

then check the following relation for every p_i.

$$f(x) \nmid x^{(p^2-1)/p_i} - 1, \tag{9}$$

where $f(x)$ is a randomly generated irreducible polynomial of degree 2 over $\mathbb{F}_p$.

On the other hand, generating an irreducible polynomial of an arbitrary degree over $\mathbb{F}_p$ is not difficult [4]. Particularly, when every factor of the degree m divides $p - 1$, it becomes quite easy. When $m = 2$ as an example, using $c \in \mathbb{F}_p$ such that $\left(\frac{c}{p}\right) = -1$,

$$f(x) = x^2 - c \tag{10}$$

becomes an irreducible polynomial over $\mathbb{F}_p$. Thus, it is more practical that the same binary sequence is generated by using some non-primitive irreducible polynomial.

3.2. Example

Let us observe a small example with $p = 7$ and $m = 2$. **Table** 1 shows the result. As introduced in the previous section, irreducible binomials such as $x^2 - 3$, $x^2 - 5$, and $x^2 - 6$ are obtained. Applying a simple substitution such as $x \leftarrow x+1$, irreducible trinomials such as $x^2 + 2x + 5$ are obtained. Among them, there are primitive or non-primitive irreducible polynomials as shown in **Table** 1.

See the row (1) of the table. In this case, $x^2 + 2x + 5$, $x^2 + 4x + 6$, and $x^2 + x + 3$ are transformed from $x^2 - 2$ and generate the same binary sequence 0100001110110100. Among these three irreducible polynomials, $x^2 + 2x + 5$ and $x^2 + x + 3$ are primitive polynomials of order $e = 7^2 - 1 = 48$. On the other hand, $x^2 + 4x + 6$ is a non-primitive polynomial of order 16, however it generates the same binary sequence.

Table 1: Binary sequence generated by primitive polynomial and irreducible polynomial with $p = 7$ and $m = 2$

	x^2-3		x^2-5		x^2-6		binary sequence $\mathcal{T}$
(1)	$x \leftarrow x+1$	x^2+2x+5	$x \leftarrow x+2$	$x^2+4x+6^{(*)}$	$x \leftarrow x+4$	x^2+x+3	0100001110110100
(2)	$x \leftarrow x+6$	x^2+5x+5	$x \leftarrow x+5$	$x^2+3x+6^{(*)}$	$x \leftarrow x+3$	x^2+6x+3	0001011011100001
(3)	$x \leftarrow x+3$	$x^2+6x+6^{(*)}$	$x \leftarrow x+6$	x^2+5x+3	$x \leftarrow x+5$	x^2+3x+5	0010000011010111
(4)	$x \leftarrow x+4$	$x^2+x+6^{(*)}$	$x \leftarrow x+1$	x^2+2x+3	$x \leftarrow x+2$	x^2+4x+5	0111010110000010

$^{(*)}$ They are non-primitive irreducible polynomials over $\mathbb{F}_7$. The others are all primitive polynomials.

3.3. Consideration

Since **Table** 1 is a small example, the primitivity of irreducible polynomial could be easily checked. However, when the characteristic p is large, the primitivity check is not always easy. According to **Table** 1, it is found that an irreducible polynomial of order 16 generates the same binary sequence generated by a certain primitive polynomial. In detail, it has been found that the non-primitive irreducible polynomials marked with $^{(*)}$ in **Table** 1 have the same order 16. The authors have tested a lot of prime numbers as the characteristic p with extension degree $m = 2$. According to the results, without any counter examples, the orders of the non-primitive polynomials have been given by $(p^2 - 1)/s$ and s is an odd prime factor of $p^2 - 1$.

4. Conclusion and future works

This paper has shown that, when the degree is restricted to 2, some non-primitive irreducible polynomials are able to generate the same binary sequence generated by a certain primitive polynomial. It means that, if the condition for the non-primitive irreducible polynomials are shown clearly, primitive polynomials are not necessary for generating maximal length sequence. As a future work, the condition should be theoretically shown.

Acknowledgments

This work has been supported by JSPS KAKENHI Grant-in-Aid for Scientific Research (A) Number 16H01723.

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] H. Nasu, Y. Nogami, Y. Morikawa, S. Kobayashi, and T. Sugimura, “Systematic Generation of An Irreducible Polynomial of An Arbitrary Degree m over $\mathbb{F}_p$ Such That $p > m$,” Convergence and Hybrid Information Technologies, Intech, pp. 303–316, 2010.