RAIRO-Theor. Inf. Appl. 47 (2013) 371–388
DOI: 10.1051/ita/2013043

Available online at:
www.rairo-ita.org

GLS: NEW CLASS OF GENERALIZED LEGENDRE SEQUENCES WITH OPTIMAL ARITHMETIC CROSS-CORRELATION *

Huijuan WANG[1], Qiaoyan WEN[2] and Jie ZHANG[3]

Abstract. The Legendre symbol has been used to construct sequences with ideal cross-correlation, but it was never used in the arithmetic cross-correlation. In this paper, a new class of generalized Legendre sequences are described and analyzed with respect to their period, distributional, arithmetic cross-correlation and distinctness properties. This analysis gives a new approach to study the connection between the *Legendre* symbol and the arithmetic cross-correlation. In the end of this paper, possible application of these sequences with optimal arithmetic cross-correlation is indicated.

Mathematics Subject Classification. 11T71, 14G50, 94A60.

1. Introduction

Many communication systems, such as code-division multiple-access systems, radar systems and synchronization systems, require sequences with low

Keywords and phrases. Arithmetic cross-correlation, *Legendre* symbol, primitive sequence, cyclically distinct.

* *This work is supported by National Natural Science Foundation of China (Grant Nos. 61170270, 61100203, 60903152, 61003286, 61121061), the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01, BUPT2011RC0505, 2011PTB-00-29, 2011RCZJ15, 2012RC0612).*

[1] The author is with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, P.R. China.
whj409@163.com

[2] The author is with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, 100876 Beijing, P.R. China

[3] The author is with School of Science, Beijing University of Posts and Telecommunications, 100876 Beijing, P.R. China

Article published by EDP Sciences

out-of-phase correlation values, so there are many results on the research of the binary sequences with optical correlation. The usual cross-correlation can be thought as the number of ones minus the number of zeros in one period of the sequence formed by adding the two sequences bit by bit modulo 2. However, for many classes of sequences, the usual notion of cross-correlation of two binary sequences is quite difficult to evaluate. Furthermore, there are fundamental limits on the sizes of families of sequences with optimal cross-correlation properties. Related to the correlation, Mandelbaum [10] investigated a notion of itself with carry (arithmetic auto-correlation) rather than bit by bit modulo 2. Mark Goresky and Andrew Klapper extended the notion of *arithmetic* auto-correlation to the arithmetic cross-correlation of two sequences and gave the concept of arithmetic Walsh transform [1, 3]. Moreover, they found that the arithmetic cross-correlation does not suffer from some of the constraints on families of sequences with good classical correlation.

In resent years, the arithmetic cross-correlation property of some balanced binary sequences with some special distribution has been studied. The *Legendre* sequence plays an important role in the research of the ordinary cross-correlation and has some important properties such as balanced and special distinct distribution, but there is no known analysis of *Legendre* symbol sequence in arithmetic cross-correlation.

In this paper, we introduce a new class of sequences constructed by the *Legendre* symbol over finite ring $Z/(p^e)$ with optimal arithmetic cross-correlation, which we call the generalized *Legendre* sequences (GLS). We make the construction based on the primitive sequences over finite ring $Z/(p^e)$, and it turns out that the GLS over the Galois ring extends the size of the family and show the optimal arithmetic cross-correlation property enjoyed by the longest sequences generated by FCSR (that is l-sequences). Furthermore, we give a new approach to construct the sequences with optimal arithmetic cross-correlation. In the study of GLS, we have been unable to use the 2-adic approach to obtain the main results, hence these results (Thms. 3.3, and 3.13) have been proven with the use of the Galois ring.

It is well known that the d-folds of the l-sequences, which can be regarded as the primitive sequences of order 1 over Galois ring $Z/(p^e)$ modulo 2, construct a family with optimal *arithmetic* cross-correlation [1]. However, a flaw of the l-sequences is the low 2-adic complexity which measures how large a feedback carry sequence generator is required to output a sequence. The GLS have large period and the size of the family is large enough to ensure the complexity of capacity. Experiments show that these sequences have merit when compared with the l-sequences, as their 2-adic complexity is approximately half their periods. It remains an open problem to prove this result.

This paper is organized as follows: In Section 2, we recall the notion of arithmetic cross-correlation and give some important properties of the primitive sequences over the Galois ring $Z/(p^e)$. In Section 3, we give the main results of this paper: first, we introduce the GLS and discuss their period and distribution property.

Next, we prove the optimal arithmetic cross-correlation property of the *GLS*. Finally, we make use of Galois ring mathematical toolkit to discuss the distinctness of the sequences in a subset of this family which reflect the distinctness property of the *Legendre* symbol sequences, and we give a simple ID-based remote mutual authentication in a multiuser environment by using the arithmetic cross-correlation. In Section 4, we conclude this paper and point out some unfinished problems.

Throughout this article, for any positive integers a and n, the sign $a(\bmod\ n)$ refers to the minimal non-negative residue of a modulo n. The sequence $\underline{s}_d = \{s_d(t)\}_{t\geq 0}$ is said to be a d-fold decimation of $\underline{s} = \{s(t)\}_{t\geq 0}$, if for every t, we have $s_d(t) = s(dt)$. We denote $\odot$ as the multiplication between vectors $\widetilde{A} = (a_1, a_2, \ldots, a_n)$ and $\widetilde{B} = (b_1, b_2, \ldots, b_n)$, $\widetilde{A} \odot \widetilde{B} = a_1 \cdot b_1 + a_2 \cdot b_2 + \ldots + a_n \cdot b_n$.

2. Preliminary

2.1. Primitive sequence over $Z/(p^e)$

Let $Z/(p^e) = \{0, 1, \ldots, p^e - 1\}$ be the residue ring of integers modulo p^e, where p is an arbitrary odd prime number and e is a positive integer. For a monic polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1x^1 + c_0$ of degree $n \geq 1$ over $Z/(p^e)$ with $f(0) \neq 0(\bmod p)$, there exists a positive integer N such that $f(x)|x^N - 1$ over $Z/(p^e)$. The least N is called the period of $f(x)$ over $Z/(p^e)$ and denoted by $per(f(x), p^e)$, which has an upper bound $p^{e-1}(p^n - 1)$.

If $per(f(x), p^e) = p^{e-1}(p^n-1)$, then the $f(x)$ is a primitive polynomial of degree n over $Z/(p^e)$. In this case, $f(x)$ mod p^i is also a primitive polynomial over $Z/(p^i)$, whose period is $per(f(x), p^i) = p^{i-1}(p^n - 1)$, $i = 1, 2, \ldots$ Especially, $f(x)$ mod p is a primitive polynomial over the prime field $GF(p)$.

The sequence $\underline{a} = \{a(t)\}_{t\geq 0}$ over $Z/(p^e)$ satisfying $a(t+n) = -(c_{n-1} \cdot a(t+n-1) + c_{n-2} \cdot a(t+n-2) + \ldots + c_0 \cdot a(t))$ mod p^e is called a linear recurring sequence over $Z/(p^e)$ generated by $f(x)$. The sequence $\underline{a}$ is called a primitive sequence of order n if $\underline{a}$ is generated by a primitive polynomial $f(x)$ and $\underline{a} \neq 0(\bmod p)$. The primitive sequence $\underline{a}$ has the least period $p^{e-1}(p^n - 1)$. Particularly, the primitive sequences over $Z/(p^e)$ have the following propositions.

Proposition 2.1 [5]. *Let sequence $\underline{a} = \{a(t)\}_{t\geq 0}$ be a primitive sequence of order n over $Z/(p^e)$, then*

$$a(t) \equiv -a\left(t + \frac{p^{e-1}(p^n-1)}{2}\right) (\bmod p^e)\,.$$

Proposition 2.2 [5]. *Let sequence $\underline{a} = \{a(t)\}_{t\geq 0}$ be a primitive sequence of order n over $Z/(p^e)$, then*

$$a(t) \equiv -a\left(t + \frac{p^{e-1}(p^n-1)}{2}\right) (\bmod p)\,.$$

Let the Galois ring $R_{e,n} = GR(p^e, n)$ be the unique extension of degree n over $Z/(p^e)$. It can represented as $Z/(p^e)[x]/(f(x))$, where $f(x)$ is a basic irreducible polynomial of degree n over $Z/(p^e)$. $R_{e,n}$ is a local ring with the unique maximal ideal $p \cdot R_{e,n}$. The set of units $R^*_{e,n} = R_{e,n} \setminus (p \cdot R_{e,n})$ is a multiplicative group. Let η be a generator of the cyclic group of $R^*_{e,n}$ corresponding to $Z/(p^n - 1)$. Define $\Omega_{e,n} = \{0, 1, \eta, \dots, \eta^{p^n-2}\}$, it can be shown that every element $\alpha \in GR(p^e, n)$ has a unique p-adic expansion

$$\alpha = \alpha_0 + \alpha_1 \cdot p + \ldots + \alpha_{e-1} \cdot p^{e-1},$$

where $\alpha_i \in \Omega_{e,n}$ for $i = \{0, 1, 2, \dots, e-1\}$. Let σ be the Frobenius map from $GR(p^e, n)$ to $GR(p^e, n)$ given by

$$\sigma(\alpha) = \alpha_0^p + \alpha_1^p \cdot p + \ldots + \alpha_{e-1}^p \cdot p^{e-1}.$$

As we know σ is the generator of the Galois group of $GR(p^e, n)/(Z/(p^e))$, which is a cyclic group of order n. The trace mapping $\mathrm{Tr}(\cdot) : GR(p^e, n) \longrightarrow Z/(p^e)$ is defined as follows

$$\mathrm{Tr}(x) = x + \sigma(x) + \ldots + \sigma^{n-1}(x),$$

for $x \in GR(p^e, n)$.

If $f(x)$ is a primitive polynomial over $Z/(p^e)$ with degree n, let $\xi \in GR(p^e, n)$ be a root of $f(x)$. Then, for any primitive sequence $\underline{a}$ which is generated from $f(x)$, there must exist a unique $\alpha \in R^*_{e,n}$ such that

$$a(t) = \mathrm{Tr}\left(\alpha \cdot \xi^t\right)$$

for $t \geq 0$. As we know, the order of ξ is $p^{e-1}(p^n - 1)$. So ξ can be written as $\xi = \eta(1 + p\eta_1)$, where η is a generator of $\Omega_{e,n}$ and $\eta_1 \in R^*_{e,n}$. We denote $\Gamma_n = \{1, \xi, \xi^2, \dots, \xi^{p^{e-1}(p^n-1)-1}\}$.

Assume the polynomial $P(x) = x^n - r$ is irreducible in $Z/(p^e)$, and the polynomial $c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$, $(c_i \in Z/(p^e))$, modulo $P(x)$ form a Galois ring $GR(p^e, n)$.

Let $\xi \in GR(p^e, n)$ be a root of the primitive polynomial $f(x)$. For every $\xi^t \in GR(p^e, n)$, $t \geq 0$, we can find $c_{jt} \in Z/(p^e)$ for $j = 0, 1, 2, \dots, n-1$ to denote $\xi^t = c_{0t} + c_{1t} \cdot x + c_{2t} \cdot x^2 + \ldots + c_{(n-1)t} \cdot x^{n-1}$. Any element $c_{jt} \in Z/(p^e)$ has a unique p-adic decomposition as $c_{jt} = c_{jt,0} + c_{jt,1} \cdot p + c_{jt,2} \cdot p^2 + \ldots + c_{jt,e-1} \cdot p^{e-1}$, where $c_{jt,i} \in Z/(p)$, $i = 0, 1, \dots, e-1$. Then

$$\xi^t = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{e-1} c_{jt,i} \cdot p^i \right) \cdot x^j = \sum_{i=0}^{e-1} \left(\sum_{j=0}^{n-1} c_{jt,i} \cdot x^j \right) \cdot p^i$$

is also the p-adic expansion. So the polynomials $\sum_{j=0}^{n-1} c_{jt,i} \cdot x^j$, $i = 0, 1, 2, \dots, e-1$, can be regarded as the elements in $\Omega_{e,n}$. Since the trace mapping $\mathrm{Tr}(\cdot)$ is from

$GR(p^e, n)$ to $Z/(p^e)$, we assume the function $\mathrm{tr}(\cdot)$ as

$$\mathrm{tr}\left(\sum_{j=0}^{n-1} c_{jt,i} \cdot x^j\right) = \sum_{k=0}^{n-1}\left(\sum_{j=0}^{n-1} c_{jt,i} \cdot x^j\right)^{p^k}$$

is a mapping from $\Omega_{e,n}$ to $Z/(p)$.

Then the trace mapping $\mathrm{Tr}(\xi^t) : GR(p^e, n) \longrightarrow Z/(p^e)$ can be represented as:

$$\mathrm{Tr}(\xi^t) = \mathrm{tr}\left(\sum_{j=0}^{n-1} c_{jt,0} \cdot x^j\right) + \mathrm{tr}\left(\sum_{j=0}^{n-1} c_{jt,1} \cdot x^j\right) \cdot p + \ldots + \mathrm{tr}\left(\sum_{j=0}^{n-1} c_{jt,e-1} \cdot x^j\right) \cdot p^{e-1}.$$

Similar to the trace mapping from $GF(p^n)$ to $Z/(p)$, we denote

$$\mathrm{tr}\left(\sum_{j=0}^{n-1} c_{jt,i} \cdot x^j\right) = n \cdot c_{0t,i}.$$

When n is relatively prime with p, the trace mapping $\mathrm{Tr}(\xi^t) : GR(p^e, n) \longrightarrow Z/(p^e)$ can be written as

$$\mathrm{Tr}(\xi^t) = n \cdot c_{0t,0} + n \cdot c_{0t,1} \cdot p + \ldots + n \cdot c_{0t,e-1} \cdot p^{e-1} = n \cdot c_{0t}. \qquad (2.1)$$

2.2. 2-Adic integer and arithmetic cross-correlation

In this subsection, we briefly review some basic facts about the 2-adic integer and recall the notion of the Arithmetic Cross-correlation.

Let binary sequence $\underline{s} = s(0), s(1), s(2), s(3), \ldots$ have least period T with pre-period t_0, so that $s(t + T) = s(t)$ with $t \geq t_0$. If $t_0 > 0$ we denote the sequence $\underline{s}$ as an eventually periodic sequence, if $t_0 = 0$ we denote the sequence $\underline{s}$ as a strictly periodic sequence.

A 2-adic integer is a formal power series $\varpi = \sum_{t=0}^{\infty} s(t) \cdot 2^t$, with $s(t) \in \{0, 1\}$. The set Z_2 of the 2-adic integers forms a ring under the operations of addition and multiplication with carry. We denote the string $000\ldots$ as merely 0, and the string $100\ldots$ as 1. Besides, we must define that $1 + 2 + 2^2 + \ldots = -1$; that is, the infinite string $111\ldots$ is a base-2 expansion of a negative integer -1.

Specifically, addition of the 2-adic integers is given by

$$\sum_{t=0}^{\infty} s_1(t) \cdot 2^t + \sum_{t=0}^{\infty} s_2(t) \cdot 2^t = \sum_{t=0}^{\infty} s_3(t) \cdot 2^t,$$

if there are carry integers $d_0, d_1, d_2, \ldots$ such that $d_0 = 0$, and for all $t \geq 0$, we have $s_1(t) + s_2(t) = s_3(t) + 2d_{t+1} - d_t$.

Similarly, the multiplication of the 2-adic integers is given by

$$\sum_{t=0}^{\infty} s_1(t) \cdot 2^t \cdot \sum_{t=0}^{\infty} s_2(t) \cdot 2^t = \sum_{t=0}^{\infty} s_3(t) \cdot 2^t,$$

if there are carry integers $d_0, d_1, d_2, \ldots$ such that $d_0 = 0$, and for all $t \geq 1$, we have $s_1(t) \cdot s_2(0) + s_1(t-1) \cdot s_2(1) + \ldots + s_1(0) \cdot s_2(t) = s_3(t) + 2d_{t+1} - d_t$. Note that in the Z_2, we have $-1 = 1 + 2 + 2^2 + \ldots$ The corresponding subtraction of the 2-adic numbers is

$$\sum_{t=0}^{\infty} s_1(t) \cdot 2^t - \sum_{t=0}^{\infty} s_2(t) \cdot 2^t = \sum_{t=0}^{\infty} s_1(t) \cdot 2^t + \sum_{t=0}^{\infty} 2^t \cdot \sum_{t=0}^{\infty} s_2(t) \cdot 2^t.$$

It follows that Z_2 contains all the integers. Let $q = 1 + q_1 2 + q_2 2^2 + \ldots + q_r 2^r$ be an odd integer, then the negative integer $-q$ is associated to the product

$$-q = (1 + 2 + 2^2 + 2^3 + \ldots) \left(1 + q_1 2 + q_2 2^2 + \ldots + q_r 2^r\right).$$

In Z_2, the formal power series $-q$ has a unique (multiplicative) inverse

$$(-q)^{-1} = 1 \cdot 2^0 + b_1 \cdot 2^1 + b_2 \cdot 2^2 + +b_3 \cdot 2^3 + \ldots$$

Thus the ring Z_2 contains every rational number $\frac{h}{q}$ provided q is odd.

Proposition 2.3 [9]**.** *There is a one-to-one correspondence between rational numbers $\varpi = \frac{h}{q}$ (where q is an odd number) and eventually periodic binary sequences $\underline{s}$, which associates to each rational number ϖ and the bit sequence $\underline{s} = s(0), s(1), s(2), \ldots$ of its 2-adic expansion. The sequence $\underline{s}$ is strictly periodic if and only if $\varpi \leq 0$ and $|\varpi| < 1$.*

In this correspondence, we use the operations in Z_2 to introduce the arithmetic cross-correlation. Recall that the ordinary cross-correlation with shift τ of two strictly sequences $\underline{s}_1$ and $\underline{s}_2$ of period T can be defined either as the sum $\sum_{t=0}^{T-1}(-1)^{s_1(t)+s_2(t+\tau)}$ or as the number of zeros minus the number of ones in one period of the bitwise exclusive-or of $\underline{s}_1$ and the τ shift of $\underline{s}_2$, where the τ shift of $\underline{s}_2$ is denote as $\underline{s}_2^{\tau} = s_2(0+\tau), s_2(1+\tau), s_2(2+\tau), \ldots$ The arithmetic cross-correlation is the with-carry analog, and is given by the following definition.

Definition 2.4 [1]**.** Let $\underline{s}_1$ and $\underline{s}_2$ be two strictly binary periodic sequences with period T, and let $0 \leq \tau < T$ and $\underline{s}_2^{\tau}$ be the τ shift of $\underline{s}_2$. Denote ϖ_1 and ϖ_2^{τ} as the 2-adic integers corresponding to the sequences $\underline{s}_1$ and $\underline{s}_2^{\tau}$. Then, the corresponding sequence $\underline{s}_3$ of $\varpi_1 - \varpi_2^{\tau}$ is strictly periodic or eventually periodic, and its period divides T. The shift arithmetic cross-correlation $C^a_{\underline{s}_1,\underline{s}_2}(\tau)$ of $\underline{s}_1$ and $\underline{s}_2$ is the number of zeros minus the number of ones in one period of length T of $\underline{s}_3$.

As in Definition 2.4, it is shown that the arithmetic cross-correlation of strictly periodic sequences $\underline{s}_1$ and $\underline{s}_2$ satisfy $C^a_{\underline{s}_1,\underline{s}_2} = \sum_{t=0}^{T}(-1)^{s_3(t)}$, where $\sum_{t=0}^{\infty} s_1(t) \cdot 2^t + \sum_{t=0}^{\infty} s_2(t) \cdot 2^t = \sum_{t=0}^{\infty} s_3(t) \cdot 2^t$.

If $\underline{s}_1$ and $\underline{s}_2^{\tau}$ are distinct for all $\tau \geq 0$, then $\underline{s}_1$ and $\underline{s}_2$ are cyclically distinct. If $\underline{s}_1$ and $\underline{s}_2$ are cyclically distinct and satisfy $C^a_{\underline{s}_1,\underline{s}_2}(\tau) = 0$, then $\underline{s}_1$ and $\underline{s}_2$ are said to have optimal arithmetic cross-correlation.

For instance, the sequences $\underline{s}_1 = 111101000010011101100010111101000010111101100010011101000010\ldots$ and $\underline{s}_2 = 010011011001001101100100110110010011011001001101100100110110\ldots$ have optimal arithmetic cross-correlation have optimal arithmetic cross-correlation as $\underline{s}_1 - \underline{s}_2$ has the balanced property over a period in the 2-adic ring. $\underline{s}_1 - \underline{s}_2 = \varpi_1 - \varpi_2$ as the operation in Z_2.

3. Main results

3.1. Sequences

In this subsection, we describe the main definition and derive the distribution property of generalized *Legendre* sequences (GLS).

The construction of GLS is based on the primitive sequences $\underline{a}$ of order n over $Z/(p^e)$, let $\underline{a} = \{a(t)\}_{t\geq 0}$ where $a(t) \in Z/(p^e)$. We first classify the $a(t)$,

$$C_0 = \{a(t) \in Z/(p^e) \mid a(t)(\mathrm{mod} p) = 0, \;\; t(\mathrm{mod} 4) = 0 \; or \; t(\mathrm{mod} 4) = 3\},$$

$$C_1 = \{a(t) \in Z/(p^e) \mid a(t)(\mathrm{mod} p) = 0, \;\; t(\mathrm{mod} 4) = 1 \; or \; t(\mathrm{mod} 4) = 2\},$$

$$D_0 = \{a(t) \in Z/(p^e) \mid a(t)(\mathrm{mod} p) \neq 0, \\ a(t) \; is \; the \; quadratic \; residue \; over \; Z^*/(p^e)\},$$

$$D_1 = \{a(t) \in Z/(p^e) \mid a(t)(\mathrm{mod} p) \neq 0, \\ a(t) \; is \; the \; quadratic \; non-residue \; over \; Z^*/(p^e)\}.$$

For an element a over $Z^*/(p^e)$, if there exists a non-zero square b^2 satisfying $a \equiv b^2 \bmod p^e$, we refer to a as a quadratic residue over $Z^*/(p^e)$, else a is a quadratic non-residue over $Z^*/(p^e)$.

Next, we give the notion of the generalized *Legendre* sequence (GLS).

Definition 3.1. (GLS) Let $\underline{a} = \{a(t)\}_{t\geq 0}$ be a primitive sequence of order n over $Z/(p^e)$, the generalized *Legendre* sequence $\underline{s} = \{s(t)\}_{t\geq 0}$ is denoted as

$$s(t) = \begin{cases} 1, & a(t) \in C_0 \bigcup D_0, \\ 0, & a(t) \in C_1 \bigcup D_1 \end{cases} .$$

The generalized *Legendre* sequence $\underline{s} = \{s(t)\}_{t\geq 0}$ is a binary periodic sequence.

We give a notation of a power character χ_l over $\mathit{\Gamma}_n$. Let ξ be a root of a primitive polynomial $f(x)$ of degree n over $Z/(p^e)$ (n is relatively prime with p), and it is a generator in $\mathit{\Gamma}_n$. For another element $\zeta \in \mathit{\Gamma}_n$, let $ind(\zeta)$ be the least non-negative integer k such that $\xi^k = \zeta$ and β be a primitive fourth root of unity. We denote

$$\chi_l(\zeta) = \beta^{ind(\zeta)}.$$

As ξ is a generator of Γ_n, $\xi^{p^{e-1}(p^n-1)} = (\xi^{\frac{p^n-1}{p-1}})^{p^{e-1}(p-1)} = 1$, so $\xi^{\frac{p^n-1}{p-1}}$ is an element in $Z^*/(p^e)$, where $Z^*/(p^e)$ is the maximal multiplicative group in $Z/(p^e)$. If the p and n satisfy $4|p-1$ and 2 is the biggest even divisor of n , it follows that β is an element in $Z^*/(p^e)$. Then from the equation (1) and the above analysis, we have a function χ from $Z/(p^e)$ to $Z/(p^e)$ as

$$\chi(\mathrm{Tr}(\xi^t)) = \chi(n \cdot c_{0t}) = \begin{cases} \chi_l(n \cdot c_{0t}), & n \cdot c_{0t}(\mathrm{mod} p) \neq 0 \\ \beta^t, & n \cdot c_{0t}(\mathrm{mod} p) = 0. \end{cases}$$

If $n \cdot c_{0t}(\mathrm{mod} p) \neq 0$, then $\chi(n \cdot c_{0t}) = \chi_l(n \cdot c_{0t}) = \beta^{\frac{p^n-1}{p-1} \cdot j} = (-1)^j(\mathrm{mod}\ p^e)$, where $n \cdot c_{0t} = \xi^{\frac{p^n-1}{p-1} \cdot j}$. If $n \cdot c_{0t}(\mathrm{mod} p) = 0$, there is $\chi(n \cdot c_{0t}) = \beta^t \in Z^*/(p^e)$. Consequently, $\beta^{\frac{p^n-1}{p-1} \cdot j} = (-1)^j(\bmod p^e)$ reduces to the *Legendre* symbol in $Z/(p^e)$ defined $\chi_l(a(t)) = -1$ *or* 1 according to whether $a(t)$ is a non-zero square or a non-square in $Z^*/(p^e)$. Then the generalized *Legendre* sequence $\underline{s}$ has another representation.

Lemma 3.2. *Let ξ be a root of the primitive polynomial $f(x)$ of degree n over $Z/(p^e)$ and let $\underline{a} = \{a(t)\}_{t\geq 0} = \{\mathrm{Tr}(\xi^t)\}_{t\geq 0}$ be a primitive sequence generated from $f(x)$. We have a binary sequence*

$$\underline{s} = \{s(t)_{t\geq 0}\} = \chi(a(t))(\mathrm{mod} 2).$$

Then the sequence $\underline{s}$ is the generalized Legendre sequence (GLS).

Next, we give the main result of this subsection.

Theorem 3.3. *Let $\underline{s}$ be a generalized Legendre sequence generated from a primitive sequence $\underline{a}$ of order n ($n \geq 2$) over $Z/(p^e)$. If the prime number p satisfies $4|p-1$ and 2 is the biggest even divisor of n , then the sequence $\underline{s}$ has a period $T = 2 \cdot p^{e-1} \cdot (\frac{p^n-1}{p-1})$, and the second half of the period T of $\underline{s}$ is the bitwise complement of the first half.*

Proof. As p satisfies $4|p-1$ and 2 is the biggest even divisor of n , we have that n is an even number and is relatively prime with p. We denote $\frac{p^n-1}{p-1} = 2 \cdot k_o$, k_o is an odd integer. Let

$$\xi^t = c_{0t} + c_{1t} \cdot x + c_{2t} \cdot x^2 + \ldots + c_{n-1t} \cdot x^{n-1} = c_{0t} + \widetilde{C}_t \odot \widetilde{X},$$

where $\widetilde{C}_t = (c_{1t}, c_{2t} \ldots, c_{n-1t})$ is an $n-1$ dimension vector over $Z/(p^e)$ and $\widetilde{X} = (x, x^2 \ldots, x^{n-1})$. Assume the p-adic expansion of ξ^t is

$$\xi^t = \alpha_{t,0} + \alpha_{t,1} \cdot p + \ldots + \alpha_{t,e-1} \cdot p^{e-1}.$$

Since ξ is a root of $f(x)$ and satisfies $\xi^{p^{e-1}(p^n-1)} = 1$, that is $\xi^{p^{e-1}p^n} = \xi^{p^{e-1}}$, then $\xi^{p^{e-1}} \in \Omega_{e,n}$. Let $K = p^{e-1} \cdot (\frac{p^n-1}{2(p-1)})$, then $\xi^K \in \Omega_{e,n}$. Using the p-adic expansion of ξ^K, we denote $\xi^K = \alpha_{K,0}$, $\sigma(\xi^K) = \alpha_{K,0}^p$,. . ., $\sigma(\xi^K)^{n-1} = \alpha_{K,0}^{p^{n-1}}$.The trace function can be represented as

$$\mathrm{Tr}\left(\xi^K\right) = \alpha_{K,0} + \alpha_{K,0}^p + \ldots + \alpha_{K,0}^{p^{n-1}} = \xi^K + \xi^{K\cdot p} + \ldots + \xi^{K\cdot p^{n-1}}.$$

$\xi^{(p-1)K} = -1$ is due to $\xi^{p^{e-1}(p^n-1)} = 1$, so $\xi^{p\cdot K} = -\xi^K$, that is $\xi^{p\cdot K} + \xi^K = 0$. Then $\mathrm{Tr}(\xi^K) = 0$ for n is an even number.

Next, we assume $\xi^K = c_{1K}\cdot x + c_{2K}\cdot x^2 + \ldots + c_{n-1K}\cdot x^{n-1} = \widetilde{C}_K \odot \widetilde{X}$, where $\widetilde{C}_K = (c_{1K}, c_{2K}, \ldots, c_{(n-1)K})$, and consider the following cases.

Case 1, if $a(t) \bmod p \neq 0$.

Then $\chi(a(t)) = \chi(\mathrm{Tr}(\xi^t)) = \chi_l(n\cdot c_{0t})$, so from Lemma 3.2 the t-th bit in sequence $\underline{s}$ is $s(t) = \chi_l(n\cdot c_{0t})(\bmod 2)$. As n is relatively prime with p, $s(t)$ can be written as

$$s(t) = \chi_l(c_{0t})(\mathrm{mod}2),$$

and the element ξ^{t+K} in $\mathit{\Gamma}_n$ can be represented as $\xi^{t+K} = \xi^t\cdot\xi^K = (C_{0t} + \widetilde{C}_t \odot \widetilde{X})\cdot(\widetilde{C}_K \odot \widetilde{X})$. So we have $c_{0(t+K)} = r\cdot(\widetilde{C}_t \odot \widetilde{C}_K)$ and $\widetilde{C}_{t+K} = c_{0t}\cdot\widetilde{C}_K$. Then,

$$c_{0(t+2K)} = r\cdot(\widetilde{C}_{t+K} \odot \widetilde{C}_K) = r\cdot c_{0t}\cdot(\widetilde{C}_K \odot \widetilde{C}_K), \tag{3.1}$$

$$c_{0(t+4K)} = r\cdot c_{0(t+2K)}\cdot(\widetilde{C}_K \odot \widetilde{C}_K) = r^2\cdot c_{0t}\cdot(\widetilde{C}_K \odot \widetilde{C}_K)^2. \tag{3.2}$$

From Proposition 2.2, $a(t)(\mathrm{mod}p) \neq 0$ implies that $a(t + \frac{p^{e-1}(p^n-1)}{2})(\mathrm{mod}p) \neq 0$, that is $c_{0(t+(p-1)K)}(\mathrm{mod}p) \neq 0$. Since $4|p-1$, we find $\widetilde{C}_K \odot \widetilde{C}_K(\mathrm{mod}p) \neq 0$, so $\widetilde{C}_K \odot \widetilde{C}_K \in Z^*/(p^e)$.

From Proposition 2.1, $a(t) = -a(t + \frac{p^{e-1}(p^n-1)}{2})(\bmod p^e)$, that is $c_{0t}\cdot(1 + r^{\frac{p-1}{2}}\cdot(\widetilde{C}_K \odot \widetilde{C}_K)^{\frac{p-1}{2}})(\mathrm{mod}p^e) = 0$, so $r^{\frac{p-1}{2}}\cdot(\widetilde{C}_K \odot \widetilde{C}_K)^{\frac{p-1}{2}}(\mathrm{mod}p^e) = -1$. Then $r^{p-1}\cdot(\widetilde{C}_K \odot \widetilde{C}_K)^{p-1}(\mathrm{mod}p^e) = 1$. We get

$$r\cdot(\widetilde{C}_K \odot \widetilde{C}_K)(\mathrm{mod}p^e) = \xi^{\frac{p^n-1}{p-1}\cdot p^{e-1}}.$$

Thus $c_{0(t+2K)}(\mathrm{mod}p) \neq 0$, $c_{0(t+4K)}(\mathrm{mod}p) \neq 0$, and

$$\chi_l(r\cdot(\widetilde{C}_K \odot \widetilde{C}_K)) = \chi_l(r)\cdot\chi_l(\widetilde{C}_K \odot \widetilde{C}_K) = \chi_l(\xi^{\frac{p^n-1}{p-1}\cdot p^{e-1}}) = -1.$$

Since n is an even number and $x^n - r$ is irreducible over $Z/(p^e)$, then

$$\chi_l(r) = -1(\mathrm{mod}p^e), \qquad \chi_l(\widetilde{C}_K \odot \widetilde{C}_K) = 1(\mathrm{mod}p^e). \tag{3.3}$$

From the above analysis and equation (2), (3), (4), we know that

$$\chi_l(c_{0t}) = -\chi_l(c_{0(t+2K)}), \qquad \chi_l(c_{0t}) = \chi_l(c_{0(t+4K)}).$$

That is

$$s(t) + s(t+2K) = 1, \qquad s(t) = s(t+4K).$$

Case 2, if $a(t)(\mathrm{mod} p) = 0$. Then

$$\chi(a(t)) = \beta^t.$$

From the analysis of Case 1, it follows that $a(t+2K)(\mathrm{mod} p) = a(t+4K)(\mathrm{mod}\ p) = 0$, that is

$$\chi(a(t+2K)) = \beta^{t+2K}, \quad \chi(a(t+4K)) = \beta^{t+4K}.$$

Since K is an odd number and β is a primitive fourth root of unity, we get

$$\chi(a(t+2K)) = -\beta^t = -\chi(a(t)), \quad \chi(a(t+4K)) = \beta^t = \chi(a(t)).$$

Therefore,

$$s(t) + s(t+2K) = 1, \quad s(t) = s(t+4K).$$

So, from Case 1 and Case 2, we get that the arbitrary generalized *Legendre* sequence $\underline{s}$ has a period of length $T = 4K = 2 \cdot p^{e-1} \cdot (\frac{p^n-1}{p-1})$ and the second half of the period T of $\underline{s}$ is the bitwise complement of the first half. □

Corollary 3.4. *Let d be positive integer which is relatively prime to the period of the generalized Legendre sequence $\underline{s}$. Let $\underline{s}_d$ be a d-fold decimation of $\underline{s}$. Then, the second half of one period of $\underline{s}_d$ is the complement of the first half.*

Proof. From Theorem 3.3, the period of the sequence $\underline{s}$ is an even number, so the integer d must be an odd number and $\underline{s}_d$ has a period of $4K$. From Theorem 3.3, we know that the sequence $\underline{s}$ satisfies $s(t) + s(t+2K) = 1$. Thus

$$s_d(t) = s(td) = 1 - s(td + 2K) = 1 - s(d \cdot (t+2K)) = 1 - s_d(t+2K). \quad \square$$

We denote $F_{\underline{s}}$ as the family which contains all d-fold decimation sequences of $\underline{s}$, where d is relatively prime to the period of the sequence $\underline{s}$. In the next subsection, we will give the arithmetic cross-correlation property of the sequences in $F_{\underline{s}}$.

3.2. Arithmetic cross-correlation

For any two sequences $\underline{s}_1$ and $\underline{s}_2$ in $F_{\underline{s}}$, Corollary 3.4 shows that the second half of one period is the first half and the sequences are strictly periodic. We first need two lemmas before proving the arithmetic cross-correlation of sequences in $F_{\underline{s}}$.

Lemma 3.5. *Let $\underline{s}_1 = \{s_1(t)\}_{t\geq 0}$, $\underline{s}_2 = \{s_2(t)\}_{t\geq 0}$ be two nonzero binary periodic sequences and ϖ_1, ϖ_2 be the corresponding 2-adic integers of $\underline{s}_1$, $\underline{s}_2$. If $\varpi_1 = -\varpi_2$ and T is the common period of $\underline{s}_1$, $\underline{s}_2$, then in a period of length T the number of ones in the sequence $\underline{s}_1$ equals to the number of zeros in the sequence $\underline{s}_2$.*

Proof. Since the corresponding 2-adic integers of $\underline{s}_1$, $\underline{s}_2$ satisfy $\varpi_1 = -\varpi_2$, the sequence $\underline{s}_1$ or $\underline{s}_2$ is an eventually periodic sequence. Assume the sequence $\underline{s}_2$ is an eventually periodic sequences with period T and pre-period t_0.

Following the addition of the 2-adic integers, we get that

$$s_1(t) + s_2(t) = s_3(t) + 2d_{t+1} - d_t,$$

where $t \geq t_0$ and $s_3(t)$ is the $t-th$ bit of sequence $\underline{s}_3$ which corresponds to $\varpi_1+\varpi_2$. Since $\varpi_1 + \varpi_2 = 0$, then $s_3(t) = 0$, that is $s_1(t) + s_2(t) = 2d_{t+1} - d_t$. Thus in a period of length T we have

$$\sum_{t=t_0}^{T+t_0-1} (s_1(t) + s_2(t_0 + t)) = \sum_{t=t_0}^{T+t_0-1} (2d_{t+1} - d_t). \tag{3.4}$$

Since $\underline{s}_1$, $\underline{s}_2$ are nonzero sequences and from the properties of the addition of the 2-adic integers , we know that $d_t = 1$ for all $t \geq t_0$. That is

$$\sum_{t=t_0}^{T+t_0-1} (s_1(t) + s_2(t)) = T.$$

Thus, in a period of length T, the number of ones in the sequence $\underline{s}_1$ equals to the number of zeros in the sequence $\underline{s}_2$. □

From Theorem 3.3, we know that T is an even integer. Then the sequence $\underline{s}$ with period T can be separated into $\underline{s} = (s^1, s^2, s^1, s^2, \ldots)$, where $s^1 = (s(0), s(1), \ldots s(\frac{T}{2} - 1))$, $s^2 = (s(\frac{T}{2}), s(\frac{T}{2} + 1), \ldots s(T - 1))$. In the following analysis, let $\underline{s}^1 = (s^1, s^1, s^1, s^1, \ldots)$, $\underline{s}^2 = (s^2, s^2, s^2, s^2, \ldots)$ denote sequences with period of length $\frac{T}{2}$. The sequence $\underline{s}$ refers to the combination of $\underline{s}^1$, $\underline{s}^2$ and is denoted by $\underline{s} = (\underline{s}^1, \underline{s}^2)$.

Lemma 3.6. *Let $\underline{s}_1 = \{s_1(t)\}_{t\geq 0}$, $\underline{s}_2 = \{s_2(t)\}_{t\geq 0}$ be binary strictly periodic sequences in $F_{\underline{s}}$ with the common period of length T, and $\underline{s}_1 = (\underline{s}_1^1, \underline{s}_1^2)$, $\underline{s}_2 = (\underline{s}_2^1, \underline{s}_2^2)$. Then for all $\tau \geq 0$,*

$$C^a_{\underline{s}_1,\underline{s}_2}(\tau) = C^a_{\underline{s}_1^1,\underline{s}_2^1}(\tau) + C^a_{\underline{s}_1^2,\underline{s}_2^2}(\tau).$$

Proof. The second half of $\underline{s}_1$ and $\underline{s}_2$ are the complement of their first half. Let $\tau \geq 0$. We consider the following case.

Cases 1, if $s_1(\frac{T}{2} - 1) \neq s_2(\frac{T}{2} - 1 + \tau)$, we can assume $s_1(\frac{T}{2} - 1) = 1$ and $s_2(\frac{T}{2} - 1 + \tau) = 0$. So the minus of the $(\frac{T}{2} - 1)$-th bit in Z_2 between $\underline{s}_1$ and $\underline{s}_2^\tau$ has no effect on the following arithmetic. Then the number of zeros minus the number of ones in a period T of $\underline{s}_1 - \underline{s}_2^\tau$ is equivalent to the number of zeros minus the number of ones in a period $\frac{T}{2}$ of $\underline{s}_1^1 - \underline{s}_2^{1\tau}$ plus the number of zeros minus the number of ones in a period $\frac{T}{2}$ of $\underline{s}_1^2 - \underline{s}_2^{2\tau}$.

Cases 2, if $s_1(\frac{T}{2} - 1) = s_2(\frac{T}{2} - 1 + \tau)$, there exists a minimum integer k satisfying $s_1(\frac{T}{2} - 1 - k) \neq s_2(\frac{T}{2} - 1 - k + \tau)$. We can assume $s_1(\frac{T}{2} - 1 - k) = 1$ and $s_1(\frac{T}{2} - 1 - k + \tau) = 0$. So the $(\frac{T}{2} - 1 - k)$-th bit of the minus in Z_2 between $\underline{s}_1$ and $\underline{s}_2^\tau$ doesn't influence the following arithmetic. So we can also get that the number of zeros minus the number of ones in a period T of $\underline{s}_1 - \underline{s}_2^\tau$ is equivalent to the addition of $\underline{s}_1^1 - \underline{s}_2^{1\tau}$ and $\underline{s}_1^2 - \underline{s}_2^{2\tau}$.

From the cases 1 and 2, we find that

$$C^a_{\underline{s}_1,\underline{s}_2}(\tau) = C^a_{\underline{s}_1^1,\underline{s}_2^1}(\tau) + C^a_{\underline{s}_1^2,\underline{s}_2^2}(\tau). \qquad \square$$

Theorem 3.7. *Let* $\underline{s}_1 = \{s_1(t)\}_{t\geq 0}$*,* $\underline{s}_2 = \{s_2(t)\}_{t\geq 0}$ *be two binary strictly periodic sequences with period* T *in* $F_{\underline{s}}$*. If* $\underline{s_1}$ *and* $\underline{s}_2$ *are cyclically distinct, then* $C^a_{\underline{s}_1,\underline{s}_2}(\tau) = 0$*, for* $\tau \geq 0$*.*

Proof. Assume $\underline{s}_1 = (\underline{s}_1^1, \underline{s}_1^2)$, $\underline{s}_2 = (\underline{s}_2^1, \underline{s}_2^2)$. Since a binary periodic sequence with period $\frac{T}{2}$ has the minimal connection integer which is less or equal to $2^{\frac{T}{2}} - 1$, then we can assume $\underline{s}_1^1 = \frac{f_1}{q}$ $\underline{s}_2^{1\tau} = \frac{f_2}{q}$, where the integer q is the common connection integer of $\underline{s}_1^1$ and $\underline{s}_2^{1\tau}$ but not the least. As $\underline{s}_1$ and $\underline{s}_2$ are cyclically distinct that is $\underline{s}_1^1 \neq \underline{s}_2^{1\tau}$. Using the correspondence between the binary sequences and the 2-adic number, we get $\frac{f_1}{q} \neq \frac{f_2}{q}$.

As $\underline{s}_1^1$, $\underline{s}_2^{1\tau}$ are the complement of $\underline{s}_1^2$ and $\underline{s}_2^{2\tau}$, we have that $\underline{s}_1^2 = -1 - \frac{f_1}{q}$, $\underline{s}_2^{2\tau} = -1 - \frac{f_2}{q}$. That is

$$\underline{s}_1^1 - \underline{s}_2^{1\tau} = \frac{f_1 - f_2}{q}, \qquad \underline{s}_1^2 - \underline{s}_2^{2\tau} = -\frac{(f_1 - f_2)}{q}.$$

From Lemma 3.5, we get that in a period of length $\frac{T}{2}$ the number of ones in the sequence $\underline{s}_1^1 - \underline{s}_2^{1\tau}$ equals to the number of zeros in the sequence $\underline{s}_1^2 - \underline{s}_2^{2\tau}$. That is $C^a_{\underline{s_1^1},\underline{s_2^1}}(\tau) + C^a_{\underline{s}_1^2,\underline{s}_2^2}(\tau) = 0$. Thus, from Lemma 3.6,

$$C^a_{\underline{s}_1,\underline{s}_2}(\tau) = C^a_{\underline{s_1^1},\underline{s_2^1}}(\tau) + C^a_{\underline{s}_1^2,\underline{s}_2^2}(\tau) = 0. \qquad \square$$

In the proof of this subsection, the key point of the sequences with optimal arithmetic cross-correlation is the complement property. From Proposition 2.1, we find that the primitive sequences over $Z/(p^e)$ modulo 2 also satisfy this property and the transformation is relatively simple. But the l-sequences which are the primitive sequences of order 1 over $Z/(p^e)$ modulo 2 have low 2-adic complexity. However, experiments show that the 2-adic complexity of the *GLS* is larger and is approximated by the half of the least period. But we have not been able to prove a result about the 2-adic complexity of the *GLS* and the relationships between the primitive sequences and the *GLS* have proven extremely resistant to analysis.

From Theorem 3.7, we find that the sequences in $F_{\underline{s}}$ have optimal arithmetic cross-correlation due to the balanced property of their subtraction sequence. Based on this point of view and the analysis in Lemma 3.5, we give a new approach to the study of the sequences with optimal arithmetic correlation. Because this construction has no direct relationship with the GLS, we just give a simple description in the following.

Lemma 3.8. *Let $\underline{s}_1 = \{s_1(t)\}_{t\geq 0}$, $\underline{s}_2 = \{s_2(t)\}_{t\geq 0}$ be two binary strictly periodic sequences with a common period of length T and with corresponding 2-adic integers ϖ_1, ϖ_2. Then there must exist another two binary strictly periodic sequences $\underline{s}_3 = \{s_3(t)\}_{t\geq 0}$, $\underline{s}_4 = \{s_4(t)\}_{t\geq 0}$ with the common period of length T and corresponding 2-adic integers ϖ_3, ϖ_4 that satisfy*

$$\varpi_3 - \varpi_4 = \varpi_2 - \varpi_1.$$

Proof. This is easy to derive from the operation of sequences in the 2-adic ring. □

Let $\underline{S}_1 = (\underline{s}_1, \underline{s}_3) = s_1, s_3, s_1, s_3 \ldots$, $\underline{S}_2 = (\underline{s}_2, \underline{s}_4) = s_2, s_4, s_2, s_4 \ldots$, where $s_i = (s_i(0), s_i(2), \ldots, s_i(T-1))$, $i = 1, 2, 3, 4$. From Lemma 3.8, the sequence $\underline{s}_1 - \underline{s}_2$ and $\underline{s}_2 - \underline{s}_4$ must be an eventually periodic sequence. Thus, there must exist sequences $\underline{s}_1$, $\underline{s}_2$, $\underline{s}_3$, $\underline{s}_4$ with $s_1(0) = s_3(0) = 1$ and $s_2(0) = s_4(0) = 0$ that satisfy Lemma 3.8. Then the arithmetic correlation of $\underline{S}_1$ and $\underline{S}_2$ is given as follows.

Theorem 3.9. *Let $\underline{s}_1$,$\underline{s}_2$,$\underline{s}_3$,$\underline{s}_4$ be the cyclically distinct sequences as described in Lemma 3.8 and the sequences $\underline{S}_1 = (\underline{s}_1, \underline{s}_3)$, $\underline{S}_2 = (\underline{s}_2, \underline{s}_4)$. If $s_1(0) = s_3(0) = 1$ and $s_2(0) = s_4(0) = 0$, then*

$$C^a_{\underline{S}_1, \underline{S}_2}(0) \in \{0,\ 4,\ -4\}.$$

Proof. The arithmetic correlation of sequences $\underline{S}_1$, $\underline{S}_2$ is the number of zeros minus the number of ones in one period of length T of $\underline{S}_1 - \underline{S}_2$. Since $s_1(0) = s_3(0) = 1$ and $s_2(0) = s_4(0) = 0$, we know that the sequence $\underline{S}_1 - \underline{S}_2$ is equal to the combined $(\underline{s}_1 - \underline{s}_2, \underline{s}_3 - \underline{s}_4)$, apart from two bits that are flipped. Thus, from the definition of arithmetic correlation, we have

$$C^a_{\underline{S}_1, \underline{S}_2}(0) \in \{C^a_{\underline{s}_1, \underline{s}_2}(0) + C^a_{\underline{s}_3, \underline{s}_4}(0),\ C^a_{\underline{s}_1, \underline{s}_2}(0) + C^a_{\underline{s}_3, \underline{s}_4}(0) \pm 4\}.$$

From Lemma 3.5, we get $C^a_{\underline{s}_1, \underline{s}_2}(0) + C^a_{\underline{s}_3, \underline{s}_4}(0) = 0$. □

In the analysis of Theorem 3.9, we find that sequences without the bitwise complement property also satisfy optimal arithmetic correlation. For instance, the sequences $\underline{S}_1 = (\underline{s}_1, \underline{s}_3)$, where $\underline{s}_1 = 1, 0, 0, 1, 0, 1, 0, 0, \ldots, \underline{s}_3 = 1, 0, 0, 1, 0, 1, 1, 1, \ldots$, $\underline{S}_2 = (\underline{s}_2, \underline{s}_4)$,where $\underline{s}_2 = 0, 1, 0, 0, 0, 1, 1, 1, \ldots, \underline{s}_4 =, 0, 1, 1, 0, 1, 1, 1, 0, \ldots$, do not have the second half of the period being the bitwise complement of the first half but their subtraction sequence in the 2-adic ring has the balanced property, so their arithmetic correlation is 0.

When two sequences $\underline{s}_1$, $\underline{s}_2$ in $F_{\underline{s}}$ are cyclically distinct, the arithmetic cross-correlation of $\underline{s}_1$ and $\underline{s}_2$ is 0. When $\underline{s}_1$ and $\underline{s}_2$ are not cyclically distinct, their arithmetic cross-correlation equals to the period T. In the next subsection, we consider the cyclically distinct properties of class $F_{\underline{s}}$.

3.3. Distinctness

In this subsection, we restrict $p > 7$ to prove the cyclically distinct property of the sequences with optimal arithmetic correlation in a subset of $F_{\underline{s}}$. Before showing the main result (Thm. 4), we first list some necessary lemmas.

Lemma 3.10 [5]. *Let p be an odd prime and $e \geq 2$. Suppose $f(x)$ and $g(x)$ are two different primitive polynomials of degree n over $Z/(p^e)$ satisfying $f(x)(\mathrm{mod} p) \neq g(x)(\bmod p)$. Then for any two linear recurring sequences $\underline{u}$, $\underline{v}$ over $Z/(p^e)$ respectively generated by $f(x)$ and $g(x)$, we have $\underline{u}(\mathrm{mod} p)$ and $\underline{v}(\mathrm{mod} p)$ are cyclically distinct.*

Lemma 3.11 [5]. *Let $\underline{a}$ be a primitive sequence over $Z/(p^e)$ of degree n, and assume the sequence $\underline{a}^{'}$ is the S-fold sequence of $\underline{a}$, where $S = p^{e-1}$. Then $\underline{a}^{'}(\bmod p)$ is an m-sequence over $Z/(p)$ of degree n.*

Denote $F_{\underline{a}}$ is the class of d-fold decimation sequences of primitive sequence $\underline{a}$, where d is relatively prime to the period of $\underline{a}$ and $d < 2 \cdot \frac{p^n-1}{p-1}$. From Definition 3.1, we denote the class of generalized *Legendre* sequences generated from $F_{\underline{a}}$ as $L_{\underline{s}}$, which is a subset of $F_{\underline{s}}$. From Theorem 3.7, we know that the arithmetic correlation of the cyclically distinct sequences in $L_{\underline{s}}$ is 0. We denote the product of two periodic sequences $\underline{a}_1$, $\underline{a}_2$ in $F_{\underline{a}}$ as $\underline{a}_1 \cdot \underline{a}_2 = \{a_1(t) \cdot a_2(t)(\mathrm{mod} p^e)\}_{t \geq 0}$.

Lemma 3.12. *Let $\underline{a}_1^{'}$, $\underline{a}_2^{'}$ be the S-fold sequences of $\underline{a}_1$, $\underline{a}_2$ in $F_{\underline{a}}$, and $\underline{s}_1^{'}$, $\underline{s}_2^{'}$ be the S-fold sequences of the generalized Legendre sequences $\underline{s}_1$, $\underline{s}_2$ as generated by $\underline{a}_1$, $\underline{a}_2$, where $S = p^{e-1}$. If $\underline{a}_1^{'}(\mathrm{mod} p) \neq \underline{a}_2^{'}(\mathrm{mod} p)$, then $\underline{s}_1^{'} \neq \underline{s}_2^{'}$.*

Proof. Let the sequences $\underline{a}_1$ and $\underline{a}_2$ be the $d_1 - fold$ and $d_2 - fold$ of the primitive sequence $\underline{a}$, d_1, d_2 are relatively prime to the period of sequence $\underline{a}$ and $d_1 < 2 \cdot \frac{p^n-1}{p-1}$, $d_2 < 2 \cdot \frac{p^n-1}{p-1}$, and $\underline{a}_1^{'}$, $\underline{a}_2^{'}$ are the S-fold sequences of $\underline{a}_1$, $\underline{a}_2$. Then we can denote

$$\underline{a}_1^{'} = \{a_1^{'}(t)\}_{t \geq 0} = \{a_1(S \cdot t)\}_{k \geq 0},$$

$$\underline{a}_2^{'} = \{a_2^{'}(t)\}_{t \geq 0} = \{a_2(S \cdot t)\}_{k \geq 0}.$$

So the sequences $\underline{a}_1^{'}$ and $\underline{a}_2^{'}$ have the least period of length $p^n - 1$. From Lemma 3.11, we know that the sequences $\underline{a}_1^{'}(\bmod p)$, $\underline{a}_2^{'}(\bmod p)$ are the m-sequences over $Z/(p)$ of degree n. Next, we assume $\underline{a}_1^{'}(\mathrm{mod} p) \neq \underline{a}_2^{'}(\mathrm{mod} p)$.

Let $\underline{s}_1$ and $\underline{s}_2$ be two sequences in $L_{\underline{s}}$ generated by the sequences $\underline{a}_1$ and $\underline{a}_2$ respectively. Assume $\underline{s}_1^{'}$, $\underline{s}_2^{'}$ are the S-fold sequences of $\underline{s}_1$, $\underline{s}_2$. From Theorem 3.3, we know that sequences $\underline{s}_1^{'}$, $\underline{s}_2^{'}$ have period of length

$$T^{'} = \frac{2 \cdot (p^n - 1)}{p - 1}.$$

Next, we consider a string of length $T^{'} = \frac{2 \cdot (p^n-1)}{p-1}$ in the sequence $\underline{a}_1^{'} \cdot \underline{a}_2^{'}$, where $T^{'} = P_0 + P_1 + P_{-1}$, and P_0 is the number of t satisfying $a_1^{'}(t) \cdot a_2^{'}(t)(\mathrm{mod} p) = 0$

in this string, P_1 is the number of t satisfying $\chi_l(a_1^{'}(t) \cdot a_2^{'}(t)(\mathrm{mod} p^e)) = 1$ and P_{-1} is the number of t satisfying $\chi_l(a_1^{'}(t) \cdot a_2^{'}(t)(\mathrm{mod} p^e)) = -1$.

Since $\underline{a}_1^{'}(\mathrm{mod} p)$, $\underline{a}_2^{'}(\mathrm{mod} p)$ are the m-sequences over $Z/(p)$ of degree n, from the property of the m-sequence, we know that the number of $a_1^{'}(t)(\mathrm{mod} p) = 0$ and $a_2^{'}(t)(\mathrm{mod} p) = 0$ is $p^{n-1} - 1$. So the number of $a_1^{'}(t) \cdot a_2^{'}(t)(\mathrm{mod} p) = 0$ in a period of length $p^n - 1$ of sequence $\underline{a}_1^{'} \cdot \underline{a}_2^{'}$ is at most $2 \cdot (p^{n-1} - 1)$. So in the sequence $\underline{a}_1^{'} \cdot \underline{a}_2^{'}$, we can assume that the first $\frac{2 \cdot (p^n - 1)}{p-1}$ length of this sequence satisfy

$$P_0 \leq \frac{4 \cdot (p^{n-1} - 1)}{p-1}.$$

From Definition 3.1 and Lemma 3.2, we know that P_1 equals the number of t with $s_1^{'}(t) \oplus s_2^{'}(t) = 0$. From the above analysis of Theorem 3.3, the sequences $\underline{s}_1^{'}$, $\underline{s}_2^{'}$ have period $\frac{2 \cdot (p^n - 1)}{p-1}$, and the correlation of the *Legendre* sequences generated by $\underline{a}_1^{'}$, $\underline{a}_2^{'}$ is no more than $2 \cdot (p^{n-1} - 1)$. So the integer P_1 is at most $\frac{p^n - p^{n-1}}{p-1} + \frac{4 \cdot (p^{n-1} - 1)}{p-1}$. That is

$$P_1 \leq \frac{p^n - p^{n-1}}{p-1} + \frac{4 \cdot (p^{n-1} - 1)}{p-1}.$$

Since

$$T^{'} - P_0 - P_1 = P_{-1} > 0,$$

so there must exist an integer t in the first string of length $T^{'}$ of sequence $\underline{a}_1^{'} \cdot \underline{a}_2^{'}$ satisfying

$$\chi_l(a_1^{'}(t) \cdot a_2^{'}(t)(\mathrm{mod} p^e)) = -1,$$

where $a_1^{'}(t) \cdot a_2^{'}(t)(\mathrm{mod} p) \neq 0$.

As $\chi_l(a_1^{'}(t) \cdot a_2^{'}(t)(\mathrm{mod} p^e)) = \chi_l(a_1^{'}(t))(\mathrm{mod} p^e) \cdot \chi_l(a_2^{'}(t))(\mathrm{mod} p^e)$, we have

$$s_1^{'}(t) \neq s_2^{'}(t).$$

Then we arrive at $\underline{s}_1^{'} \neq \underline{s}_2^{'}$. □

Theorem 3.13. *Let sequence $\underline{a} = \{a(t)\}_{t \geq 0}$ be a primitive sequence of order n ($n \geq 2$) over $Z/(p^e)$ where $p > 7$ satisfying $4|p-1$ and 2 is the biggest even divisor of n. If $\underline{a}_1$, $\underline{a}_2$ are two different sequences in $F_{\underline{a}}$ and their primitive generator polynomials $f(x)$ and $g(x)$ satisfy $f(x)(\mathrm{mod} p) \neq g(x)(\mathrm{mod} p)$, then the generalized Legendre sequences $\underline{s}_1$ and $\underline{s}_2$ are respectively generated by $\underline{a}_1$ and $\underline{a}_2$. Then $\underline{s}_1$ and $\underline{s}_2$ are cyclically distinct.*

Proof. Since $\underline{a}_1$ and $\underline{a}_2$ are two different sequences in $F_{\underline{a}}$ and their primitive generator polynomials $f(x)$ and $g(x)$ satisfy $f(x)(\mathrm{mod} p) \neq g(x)(\mathrm{mod} p)$. Then from Lemma 3.10, the sequences $\underline{a}_1(\mathrm{mod} p)$ and $\underline{a}_2(\mathrm{mod} p)$ are cyclically distinct. Assume $\underline{a}_1^{'}$, $\underline{a}_2^{'}$ are the S-fold sequences of $\underline{a}_1$, $\underline{a}_2$, where $S = p^{e-1}$. From Lemma 3.11, we know that the sequences $\underline{a}_1^{'}(\mathrm{mod} p)$, $\underline{a}_2^{'}(\mathrm{mod} p)$ are m-sequences over $Z/(p)$ of degree n and are the S-fold decimation of sequences $\underline{a}_1(\mathrm{mod} p)$, $\underline{a}_2(\mathrm{mod} p)$. So $\underline{a}_1^{'}(\mathrm{mod} p)$ and $\underline{a}_2^{'}(\mathrm{mod} p)$ are cyclically distinct. For all $\tau \geq 0$, we have $\underline{a}_1^{'}(\text{mod}p) \neq \underline{a}_2^{'}(\tau)(\text{mod}p)$, where $\underline{a}_2^{'}(\tau)(\text{mod}p)$ is the τ-shift of sequence $\underline{a}_2^{'}(\text{mod}p)$.

Assume $\underline{s}_1^{'} = \{s_1(t_0 + S \cdot t)\}_{t\geq 0}$, $\underline{s}_2^{'}(\tau) = \{s_2(t_0 + \tau + S \cdot t)\}_{t\geq 0}$ are the S-fold sequences of the generalized *Legendre* sequences $\underline{s}_1$, $\underline{s}_2(\tau)$ as generated by $\underline{a}_1$, $\underline{a}_2(\tau)$. So there must exist an integer t_1 satisfying $s_1(t_0+S\cdot t_1) \neq s_2(t_0+S\cdot t_1+\tau)$. So for all $\tau \geq 0$, there must exist an integer $t = t_0 + S \cdot t_1$ satisfying

$$s_1(t) \neq s_2(t + \tau).$$

Then the sequences $\underline{s}_1$ and $\underline{s}_2$ are cyclically distinct. □

From Theorem 3.13, we find that the cyclically distinct sequences in $L_{\underline{s}}$ depend on their primitive generator polynomial over $Z/(p^e)$ modulo p, so $L_{\underline{s}}$ can be divided into subsets L_1, L_2,..., L_{N-1}, where the integer N denotes the number of different primitive polynomials over $Z/(p^e)$ modulo p which generate the primitive sequences in $F_{\underline{a}}$. The sequences in different subsets are cyclically distinct. Moreover, based on the proof of Lemma 3.12, we also find the following property.

Corollary 3.14. *Let $\underline{a}_1$ be a primitive sequence generated by a primitive polynomial $f(x)$ of order n over $Z/(p^{e_1})$, $\underline{a}_2$ be a primitive sequence generated by a primitive polynomial $g(x)$ of order n over $Z/(p^{e_2})$, where $e_1 \neq e_2$. The sequences $\underline{s}_1$, $\underline{s}_2$ are the generalized Legendre sequences generated by $\underline{a}_1$, $\underline{a}_2$. If $f(x)(\text{mod}p) \neq g(x)(\text{mod}p)$, then $\underline{s}_1$, $\underline{s}_2$ are cyclically distinct.*

We use these properties to give a simple ID-based remote mutual authentication in a multiuser environment. A brief description about this crypto-system is given in the following.

This scheme has two roles: one is to mutually authenticate the users $\{U_1, U_2, \ldots, U_N\}$ and a remote server A, and the second is to generate the secret key between them.

- System initializing phase:

Step 1. The server A random selects the integer pair (p, n), and integers e_1, e_2, ..., e_N, where $p > 7$ is an odd large prime satisfying $4|(p-1)$ and 2 is the biggest even factor of n.

Step 2. The server A uses the pairs (p, n, e_i), $i = 1, 2, \ldots N$, to generate the integers d_i, where the p^{e_i}-adic representation of d_i can correspond to a primitive polynomial f_i of degree n over $Z/(p^{e_i})$ and satisfy $f_i(\text{mod}p) \neq f_j(\text{mod}p)$, $i \neq j$.

Step 3. The server A keeps the key set $P = \{d_i, p, e_i, n\}$ secret.

- User registration phase:

Step 1. The user U_i chooses his identity and submits it to the server A with some personal secret information through a secure channel.

Step 2. The server A checks the identity of the user U_i and uses each public key E_i, $i = 1, 2, \ldots, N-1$, to send $E_i(d_i, p, e_i, n)$ to each user.

- Mutual authentication with key session agreement phase

Step 1. The users use their secret key D_i to compute $D_i(E_i(d_i, p, e_i, n))$ and use the integers (d_i, p, e_i, n) to generate a set L_i of GLS .

Step 2. The users U_i, U_j, $i \neq j$, randomly choose the sequences $\underline{s}_i$, $\underline{s}_j$ in set L_i, L_j to compute their arithmetic correlation $C_a(\underline{s}_i, \underline{s}_j)$. If $C_a(\underline{s}_i, \underline{s}_j) = 0$, they continue the mutual authentication, otherwise they reject the user's request.

Step 3. T The users U_i and U_j exchange the integers e_i and e_j. The user U_i computes p^{e_j} and gets a $p^{e_j} - fold$ sequence $\underline{s}_j^{'}$ of the sequence $\underline{s}_j$. If $\underline{s}_j^{'}$ has the least period of length $\frac{2\cdot(p^n-1)}{p-1}$ and the arithmetic correlation of $\underline{s}_j^{'}$ and an arbitrary p^{e_i}-fold sequence in L_i is 0, U_i confirms the validity of the user U_j, otherwise the user's request is rejected. The user U_j can authenticate U_i in the same way.

This ID-based remote mutual authentication crypto-system is just a simple example to analyze the distinct properties of the GLS and only proposes a new method for signature verifying by using arithmetic cross-correlation. The advantage over comparable traditional schemes of this system is due to the different definitions and purpose of the public keys in the user registration phase, which result in the various relative merits. But compared to other sequence schemes, the large size of the GLS increases the space complexity of the key set. We hope the applications of the arithmetic cross-correlation to communication and password encryption may find some use in future.

4. Conclusion

In this article, a new class of sequences called generalized *Legendre* sequences is introduced. Moreover, the arithmetic cross-correlation property and the distinctness of their decimation are shown. Remaining open problems include to determine period of these sequences, and to classify the sequences with respect to distinctness. Furthermore, although our experiments found that the 2-adic complexity of these sequences approximated by half of the least period, but we have not prove this.

References

[1] M. Goresky and A. Klapper, Arithmetic crosscorrelations of feedback with carry shift register sequences. *IEEE Trans. Inform. Theory* **43** (1997) 1342–C1345.

[2] Hong Xu, Wen-Feng Qi, Further results on the distinctness of decimations of l-sequences. *IEEE Trans. Inform. Theory* **52** (2006) 3831–3836.

[3] A. Klapper and M. Goresky, Arithmetic correlations and Walsh transforms. *IEEE Trans. Inform. Theory* **58** (2012) 479–492.

[4] Qun-Xiong Zheng and Wen-Feng Qi, Distribution properties of compressing sequences derived from primitive sequence over $Z/(p^e)$. *IEEE Trans. Inform. Theory* **56** (2010) 479–492.

[5] X.Y. Zhu and Wen-Feng Qi, Uniqueness of the distribution of zeroes of primitive level sequences over $Z/(p^e)$. *Finite Fields* **11** (2005) 30–44.

[6] J.-H. Kim and H.-Y. Song, Trace representation of Legendre sequences. Designs. *Codes and Cryptography* **24** (2001) 343–348.

[7] M. Goresky and A. Klapper, Fibonacci and Galois representations of feedback-with-carry shift registers. *IEEE Trans. Inform. Theory* **48** (2002) 2826–2836.

[8] Fan Shu-qin and Han Wen-bao, Distribution of elements in primitive sequences over $Z/(p^e)$. *J. Math. Res. Exposition* **24** (2004) 219–224.

[9] A. Klapper and M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory. *J. Cryptology* **10** (1997) 111–147.

[10] D. Mandelbaum, Arithmetic codes with large distance. *IEEE Trans. Inform. Theory* **IT-13** (1967) 237–242.

[11] Hong Xu and Wen-Feng Qi, Autocorrelations of maximum period FCSR sequence. *Soc. Infustrial Appl. Math.* **20** (2006) 568–577.

[12] M. Goresky and A. Klapper, Statistical Properties of the Arithmetic Correlation of Sequences. *Internat. J. Found. Comput. Sci.* **22** (2011) 1297–1315.

[13] Tian Tian and Wen-Feng Qi, 2-Adic Complexity of Binary m-sequences. *IEEE Trans. Inf. Theory* **56** (2010) 450–454.

[14] Huijuan WANG, Qiaoyan WEN and Jie ZHANG, 2-Adic Complexity of Self-shrinking Sequence. *IEEE Trans. Fundamentals* **E94-A** (2011) 11.

[15] R.A. Rueppel, *Analysis and Design of Stream ciphers (Communications and Control Engineering Series).* Springer-Verlag, Berlin, Germany (1986).

[16] R. Lidl and H. Niederriter, Finite Fields. Reading MA: Addison-Wesley (1983).

[17] Tian Tian and Wen-Feng Qi, Autocorrelation and distinctness of decimations of l-sequences based on primes. *Soc. Industrial Appl. Math.* **23** (2009) 805–821.

[18] Th.W. Cusick, Cunsheng Ding, Ari Renvall, *Stream Ciphers and Number Theory. Language Arts and Disciplines* (1998).

Communicated by D. Augot.
Received July 3, 2012. Accepted September 26, 2013.