Contemporary Mathematics

A Family of Binary Sequences from Interleaved Construction and their Cryptographic Properties

Jing Jane He, Daniel Panario, and Qiang Wang

Abstract. Families of pseudorandom sequences with low cross correlation have important applications in communications and cryptography. Among several known constructions of sequences with low cross correlations, interleaved constructions proposed by Gong uses two sequences of the same period with two-level autocorrelation. In this paper, we study the balance property and the cross correlation of interleaved sequences such that the base sequences may not have the same period, or they may not have two-level autocorrelation. In particular, we study the interleaved sequences of two Legendre sequences of periods p and q, respectively, where p and q are odd prime numbers.

1. Introduction

Pseudorandom sequences are widely used in computer science and engineering including applications to spread spectrum communication systems, radar systems, signal synchronization, simulation and cryptography [**3**]. The pseudorandom sequences in a good family should be easy to generate (possibly with hardware or software), have good distribution properties which make them appear statistically to be random, have low cross correlation values so that each sequence may be separated from the others in the family, and arise from some underlying algebraic structure so they can be analyzed using standard mathematical tools. In this paper we continue the study began in [**4**] of constructed families of sequences from interleaved structure which enjoy many nice properties. We seek families of binary sequences with low cross correlation, good randomness, and large linear complexity. Such kind of families of sequences have important applications in code-division multiple-access (CDMA) communications and cryptography [**3**]. Correlation is a measure of the similarity, or relatedness, between two phenomena. In signal processing, cross-correlation is a measure of similarity of two waveforms as a function of a time-lag applied to one of them. So the sequences with low cross correlation employed in CDMA communications can successfully combat interference from the other users who share a common channel.

1991 *Mathematics Subject Classification.* Primary 94A55; Secondary 11T06.
Key words and phrases. interleaved sequences, cross correlation.
Research of Daniel Panario and Qiang Wang is partially support by NSERC of Canada.
Version: December 14, 2009.

Let ℓ be a prime number and $\mathbb{F}_\ell$ be the finite field of ℓ elements. We consider ℓ-ary sequences which are periodic sequences with entries in $\mathbb{F}_\ell$. In particular, if $\ell = 2$, then the sequences are binary sequences. Let $\mathfrak{S}$ be a family of k ℓ-ary sequences with the same period v, and let $C_{\max}$ be the maximum magnitude of the nontrivial autocorrelation and cross correlation values of the sequences in $\mathfrak{S}$. It is known that $C_{\max} \geq v\sqrt{\frac{k-1}{vk-1}}$ which is called the Welch bound (see [**7**] or [**9**]).

Known sequences can be employed to construct new families of sequences using the interleaved structure algorithm. For example, Gong [**4**] used short two-level autocorrelation ℓ-ary sequences of period v to obtain a $(v^2, v, 2v+3)$ signal set which is optimal with respect to the Welch bound. Each sequence in this family of sequences is balanced and has large linear span. In fact, this construction can generate $v+1$ sequences so that we have a $(v^2, v+1, 2v+3)$ signal set (see page 364 in [**3**]). For $\ell = 2$, Wang and Qi [**8**] employed Legendre sequences with twin prime periods $p \equiv 3 \pmod 4$ and $p+2$ to construct a $(p(p+2), p+3, 3p+4)$ signal set, and the balance property of such family was also studied.

In this paper, we extend Gong's construction of interleaved structures where two sequences of equal length with two-level autocorrelation are used, to a general interleaved construction which uses two sequences of different length, and one sequence may not have two-level autocorrelation. In particular, we study interleaved Legendre sequences with any two odd prime periods p and q. Without loss of generality, we assume that $q \geq p$. In the case $p \equiv 3 \pmod 4$, we obtain a $\left(pq, q+1, \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)(p+1) + q\right)$ signal set which generalizes Wang and Qi's result. In the case $p \equiv 1 \pmod 4$, we obtain a $\left(pq, q+1, \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right)(p+1) + 3q - 2\right)$ signal set.

2. Preliminaries

Some notations and preliminaries for sequence construction which are used throughout the paper are given next. We introduce the terminologies about sequences in the general case, that is, most of the definitions are based on ℓ-ary sequences. Again ℓ is a prime and every element in the sequence is over $\mathbb{F}_\ell$. Later we focus on binary sequences.

Let v be a positive integer and let $\underline{a} = (a_0, \ldots, a_{v-1})$ be an ℓ-ary sequence of period v. For any integer $i \geq 0$, let the left shift operator act on $\underline{a}$ by $L^i(\underline{a}) = (a_i, a_{i+1}, \ldots, a_{i+v-1})$. In particular, define $L^\infty(\underline{a}) = (0, \ldots, 0)$.

Definition 2.1. Two sequences $\underline{a} = (a_0, \ldots, a_{v-1})$ and $\underline{b} = (b_0, \ldots, b_{v-1})$ of the same period v are called *(cyclically) shift equivalent* if there exists an integer k such that $a_i = b_{i+k}$, for all $i \geq 0$. In this case, we write $\underline{a} = L^k(\underline{b})$, or simply $\underline{a} \sim \underline{b}$. Otherwise, they are called *cyclically shift distinct*.

Definition 2.2. The *cross correlation function* $C_{\underline{a},\underline{b}}(\tau)$ of two ℓ-ary sequences $\underline{a}$ and $\underline{b}$ of period v is defined in [**2**] as

$$C_{\underline{a},\underline{b}}(\tau) = \sum_{i=0}^{v-1} \omega^{a_i - b_{(i+\tau) \pmod v}}, \quad \tau = 0, 1, \ldots,$$

where ω is a primitive ℓ-th root of unity. If $\underline{b} = \underline{a}$, then denote $C_{\underline{a}}(\tau) = C_{\underline{a},\underline{b}}(\tau)$ as the *autocorrelation* of $\underline{a}$.

DEFINITION 2.3. Let $\underline{s_j} = (s_{j,0}, s_{j,1}, \ldots, s_{j,v-1})$, $0 \le j < r$, be r shift-distinct ℓ-ary sequences of period v. Let $\mathcal{S} = \{\underline{s_0}, \ldots, \underline{s_{r-1}}\}$, and let $\delta = \max |C_{\underline{s_i},\underline{s_j}}(\tau)|$ for any $0 \le \tau < v$, $0 \le i, j < r$, where $\tau \ne 0$ if $i = j$. The set $\mathcal{S}$ is said to be a (v, r, δ) *signal set* and δ is called the *maximal correlation* of $\mathcal{S}$. We say that the set $\mathcal{S}$ has *low correlation* if $\delta \le c\sqrt{v}$ where c is a constant.

3. Algorithm for Constructing Sequences of Period $s \cdot t$

The matrix form of a sequence is an important tool to study interleaved structures.

DEFINITION 3.1. [**4**] [**5**] Fix two positive integers s and t where both s and t are not equal to 1. Given an ℓ-ary sequence $\underline{a} = (a_0, \ldots, a_{s-1})$ of period s ($\underline{a}$ is called *base sequence*) and a sequence $\underline{e} = (e_0, \ldots, e_{t-1})$, for each $0 \le i \le t-2$ such that $e_i \in \mathbb{Z}_s$ and $e_{t-1} = \infty$ ($\underline{e}$ is called *shift sequence*), let $\underline{u} = (u_0, \ldots, u_{st-1})$ be an ℓ-ary sequence of period $s \cdot t$. We arrange the elements of the sequence $\underline{u}$ into an $s \times t$ matrix as follows:

$$\mathcal{A}_u = \begin{bmatrix} u_0 & \cdots & u_{t-1} \\ \vdots & \vdots & \vdots \\ u_{(s-1)} & \cdots & u_{(s-1)t+t-1} \end{bmatrix}$$

satisfying that each column of $\mathcal{A}_u$ is a shift of $\underline{a}$. Let A_j be the j^{th} column. Then $\mathcal{A} = (A_0, \ldots, A_{t-1})$ and $A_j = L^{e_j}(\underline{a})$ and $L^{\infty}(\underline{a}) = (0, \ldots, 0)$. The matrix $\mathcal{A}_u$ is called the *matrix form of sequence* $\underline{u}$, and $\underline{u}$ is called an interleaved sequence from the base sequence $\underline{a}$ and the *shift sequence* $\underline{e}$.

Given a base sequence $\underline{a}$ and a shift sequence $\underline{e}$, an interleaved sequence $\underline{u}$ is uniquely determined. So we also say $\underline{u}$ is an (s, t)-interleaved sequence associated with $(\underline{a}, \underline{e})$. Moreover, using another sequence $\underline{b} = (b_0, \ldots, b_{s-1})$ of the same period s, Gong [**5**] constructed a family of interleaved (s, s)-sequences with the desired properties. Here we consider the case where s is not neccessarily equal to t.

ALGORITHM 3.2. Let s and t be two positive integers. Suppose that $\underline{a} = (a_0, \ldots, a_{s-1})$ and $\underline{b} = (b_0, \ldots, b_{t-1})$ are two ℓ-ary sequences of periods s and t, respectively.

(1) Choose $\underline{e} = (e_0, \ldots, e_{t-1})$ as the shift sequence for which the first $t-1$ elements are over $\mathbb{Z}_s$ and $e_{t-1} = \infty$. Moreover, if we let $d_{i-1} = e_i - e_{i-1}$, then we choose $\underline{e}$ such that $d_0, d_1 \ldots, d_{p-1}$ is in an arithmetic progression with common distance $d \ne 0$.
(2) Construct an interleaved sequence $\underline{u} = (u_0, \ldots, u_{st-1})$, whose j^{th} column in the matrix form is given by $L^{e_j}(\underline{a})$.
(3) For $0 \le i < st-1$, $0 \le j \le t$, define $\underline{s_j} = (s_{j,0}, \ldots, s_{j,st-1})$ as follow:

$$s_{j,i} = \begin{cases} u_i + b_{j+i}, & 0 \le j \le t-1, \\ u_i, & j = t. \end{cases}$$

(4) Define the family of sequences $\mathfrak{S} = \mathfrak{S}(\underline{a}, \underline{b}, \underline{e})$ as $\mathfrak{S} = \{\underline{s_j} |\ j = 0, 1, \ldots, t\}$, where $\underline{a}$ is the *first base sequence*, $\underline{e}$ is the *shift sequence*, and $\underline{b}$ is the *second base sequence*.

Because it is desirable to have more sequences in a family, without loss of generality, we can assume that $s \leq t$. We also concentrate on binary sequences ($\ell = 2$) for the rest of paper. In particular, we are interested in Legendre sequences of prime periods since they are a nice class of sequences with the randomness properties.

DEFINITION 3.3. Let p be an odd prime. The *Legendre sequence* $\underline{s} = \{s_i \mid i \geq 0\}$ of period p is defined as [**3**]

$$s_i = \begin{cases} 1, & \text{if } i \equiv 0 \pmod{p}; \\ 0, & \text{if } i \text{ is a quadratic residue modulo } p; \\ 1, & \text{if } i \text{ is a quadratic non-residue modulo } p. \end{cases}$$

The following is the known result for the autocorrelation of Legendre sequences.

PROPOSITION 3.4. [**1**]. *Let $\underline{s}$ be a Legendre sequence of prime period p as above. Then, if $p \equiv 3 \pmod 4$, $C_{\underline{s}}(\tau) = \{-1, p\}$, and if $p \equiv 1 \pmod 4$, $C_{\underline{s}}(\tau) = \{1, -3, p\}$.*

We use any two odd primes p and q to denote the periods of two Legendre sequences $\underline{a}, \underline{b}$. For similar reasons as above, we assume without loss of generality that $q \geq p$. In the following we study the family of interleaved (p, q)-sequences constructed as in Algorithm 3.2 by using Legendre sequences $\underline{a}, \underline{b}$ of periods p and q, respectively. Here we give an example of interleaved $(3, 5)$-sequence by using two Legendre sequences of period 3 and 5 respectively.

EXAMPLE 3.5.

(1) Let the first and second base sequences be Legendre sequences $\underline{a} = (1, 0, 1)$ and $\underline{b} = (1, 0, 1, 1, 0)$, respectively. We pick up a shift sequence $\underline{e} = (1, 2, 1, 1, \infty)$.

(2) We construct the interleaved sequence $\underline{u}$ associated with $\underline{a}$ and $\underline{e}$. The matrix form of $\underline{u}$ is

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

The interleaved sequence is

$$\underline{u} = (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0).$$

(3) We have

$$\begin{aligned} \underline{s_0} &= \underline{u} + \underline{b} = (111100000001000); \\ \underline{s_1} &= \underline{u} + L^1(\underline{b}) = (001011101110011); \\ \underline{s_2} &= \underline{u} + L^2(\underline{b}) = (100100110000100); \\ \underline{s_3} &= \underline{u} + L^3(\underline{b}) = (111010001101011); \\ \underline{s_4} &= \underline{u} + L^4(\underline{b}) = (000111110110101). \end{aligned}$$

(4) The family is

$$\mathfrak{S} = \{\underline{s_0}, \underline{s_1}, \underline{s_2}, \underline{s_3}, \underline{s_4}, \underline{s_5} = \underline{u}\}.$$

4. Balance Property

For any sequence $\underline{s}$, let $N_0(\underline{s})$ denote the number of zeros of the sequence $\underline{s}$.

THEOREM 4.1. *Let us choose $\underline{a}$ as the first base sequence with period v and $\underline{b}$ as the second base sequence with period w. Then using Algorithm 3.2 we construct a family $\mathfrak{S}(\underline{a}, \underline{b}, \underline{e}) = \{\underline{s_j} \mid j = 0, 1, \ldots, w\}$ with the property that the number $N_0(\underline{s_j})$ of zeros in one period of each sequence $\underline{s_j}$ is:*

$$\begin{cases} (w-1)\cdot N_0(\underline{a}) + v, & j = w; \\ N_0(\underline{a})\cdot(N_0(\underline{b})-1) + (v - N_0(\underline{a}))\cdot(w - N_0(\underline{b})) + v, & b_{j+w-1} = 0, j \le w-1; \\ N_0(\underline{a})\cdot N_0(\underline{b}) + (v - N_0(\underline{a}))\cdot(w - N_0(\underline{b}) - 1), & b_{j+w-1} = 1, j \le w-1. \end{cases}$$

PROOF. `Case 1.` $j = w$.
In this case $\underline{s_w} = \underline{u}$. Then we arrange the elements of $\underline{u}$ into the $v \times w$ matrix

$$\mathcal{A}_{\underline{u}} = [L^{e_0}(\underline{a}), \ldots, L^{e_{w-2}}(\underline{a}), \underline{0}].$$

Since each of the first $w-1$ columns is just a shift of $\underline{a}$ and $\underline{a}$ contains exactly $N_0(\underline{a})$ zeros, then the number of zeros in $\underline{u}$ is

$$N_0(\underline{u}) = (w-1)\cdot N_0(\underline{a}) + v.$$

`Case 2.` $0 \le j \le w-1$.
We denote

$$B = \begin{bmatrix} b_j & b_{j+1} & \cdots & b_{j+w-1} \\ b_j & b_{j+1} & \cdots & b_{j+w-1} \\ \vdots & \vdots & \vdots & \vdots \\ b_j & b_{j+1} & \cdots & b_{j+w-1} \end{bmatrix}.$$

Then, we have

$$\underline{s_j} = \underline{u} + L^j(\underline{b}) = \mathcal{A}_{\underline{u}} + B.$$

If $b_{j+w-1} = 0$, then there are $N_0(\underline{b}) - 1$ zeros in $b_j, \ldots, b_{j+w-2}$, and $w - N_0(\underline{b})$ ones in $b_j, \ldots, b_{j+w-2}$. So

$$N_0(\underline{s_j}) = N_0(\underline{a})\cdot(N_0(\underline{b})-1) + (v - N_0(\underline{a}))\cdot(w - N_0(\underline{b})) + v.$$

If $b_{j+w-1} = 1$, then there are $N_0(\underline{b})$ zeros in $b_j, \ldots, b_{j+w-1}$, and $w - N_0(\underline{b}) - 1$ ones in $b_j, \ldots, b_{j+w-1}$. So

$$N_0(\underline{s_j}) = N_0(\underline{a})\cdot N_0(\underline{b}) + (v - N_0(\underline{a}))\cdot(w - N_0(\underline{b}) - 1).$$

□

We observe that the number of zeros in each sequence from the constructed family is independent of the chosen shift sequence $\underline{e}$. The purpose for adding strong conditions on $\underline{e}$ is to get the desired correlation property. Wang and Qi [**8**] give the balance property of the interleaved construction with two Legendre sequences of twin prime periods p and $p+2$, respectively. However, there are some typos in their result. In the next corollary that follows immediately from the previous theorem, we give the balance property to the interleaved construction with two Legendre sequences of any two prime periods p and q which also corrects Wang and Qi's result. We remark that a Legengre sequence of length p is balanced and so it contains exactly $(p-1)/2$ zeros.

COROLLARY 4.2. Let p and q be two prime numbers and $\mathfrak{S}(\underline{a}, \underline{b}, \underline{e}) = \{\underline{s_j} \mid j = 0, 1, \ldots, q\}$ be the family of interleaved sequences constructed by Algorithm 3.2, where the base sequences $\underline{a}$ and $\underline{b}$ are Legendre sequences of period p and q respectively. Then the number of zeros $N_0(\underline{s_j})$ in one period of $\underline{s_j}$ $(0 \le j \le q)$ is

$$N_0(\underline{s_j}) = \begin{cases} \frac{p(q+1)-q+1}{2}, & j = q; \\ \frac{p(q+1)+2}{2}, & b_{j+q-1} = 0, j \le q-1; \\ \frac{p(q-1)}{2}, & b_{j+q-1} = 1, j \le q-1. \end{cases}$$

5. Cross Correlation

Gong [**4**] uses two m-sequences of the same period v to construct a family of long sequences from interleaved structures with the desired properties. Then she generalizes this idea to use several types of two-level autocorrelation sequences of period v [**5**]. Also in [**5**] the criterion for choosing the shift sequence $\underline{e} = (e_0, \ldots, e_{v-1})$ to get maximum correlation value $2v + 3$ is given like $|\{e_j - e_{j+s} \mid 0 \le j < v - s\}| = v - s$, for all $1 \le s < v$ (Theorem 2 in [**5**]). In Algorithm 3.2 we can use two sequences with different periods v and w and restrict the shift sequence $\underline{e}$ to satisfy that $e_1 - e_0, e_2 - e_1, \ldots, e_w - e_{w-1}$ is in an arithmetic progression. Before we provide the proof of the cross correlation values we need the following results.

PROPOSITION 5.1. *(Proposition 3 in* [**5**]*) Let $\underline{a}$ and $\underline{b}$ be two sequences over $\mathbb{F}_2$ of period N. For $\tau \ge 0$, we have*

(1) $< \underline{a}, \underline{b} >= C_{\underline{a},\underline{b}}(0)$;
(2) $< \underline{a}, L^\tau(\underline{b}) >= C_{\underline{a},\underline{b}}(\tau)$;
(3) $< L^i(\underline{a}), L^{j+\tau}(\underline{a}) >= C_{L^i(\underline{a}),L^j(\underline{a})}(\tau) = C_{\underline{a}}(j - i + \tau)$ *where* $i, j \ge 0$;
(4) *for* $c, d \in \mathbb{F}_2$, $< \underline{a} + c, \underline{b} + d >= (-1)^{c+d} < \underline{a}, \underline{b} >$.

In our construction, the shift sequence $\underline{e} = (e_0, \ldots, e_{w-1})$ plays an important role in computing the values of the correlation function. To determine the values of the cross correlation of the constructed sequences in $\mathfrak{S}$, we need to study the number of roots of $e_{j+s} - e_j + r \equiv 0 \pmod{v}$ for $0 \le j, s < w$, $0 \le r < v$. We observe that the index $j + s$ could go beyond the period of the shift sequence $\underline{e}$. For convenience, we introduce the extended sequence defined by $e_{j+w} = 1 + e_j$. Hence, the extended shift sequence $\underline{e}$ is $(e_0, \ldots, e_{w-2}, \infty, e_w = 1 + e_0, \ldots, e_{2w-2} = 1 + e_{w-2}, \infty)$. For the extended one, we still use the same notation $\underline{e}$ for notational convenience. In the following when encountering an element of $\underline{e}$ out of the range of the original shift sequence, we just use the extended shift sequence, i.e. $e_{j+w} = 1 + e_j$. The following proposition studies the matrix form of an interleaved sequence. It is a modification of Proposition 4 in [**5**] from $v = w$ to arbitrary v and w.

PROPOSITION 5.2. *Let $\underline{u}$ be a $(v, w)-$interleaved sequence associated with $(\underline{a}, \underline{e})$. We extend the sequence $(e_0, \ldots, e_{w-2}, \infty)$ to $\underline{e} = (e_0, \ldots, e_{2w-1})$ by defining $e_{j+w} = 1 + e_j$, for $j = 0, \ldots, w - 1$. For $\tau \ge 0$, let $T = (T_0, T_1, \ldots, T_{w-1})$ be the matrix form of $L^\tau(\underline{u})$. If we write $\tau = rw + s$, $0 \le r < v$, $0 \le s < w$ then*

$$T_j = L^{r+e_{s+j}}(\underline{a}).$$

PROOF. We use one index k for $0 \le k < vw - 1$, or two indices (i, j) for $0 \le i < v$ and $0 \le j < w$, to show the position of an element in the matrix form of

an interleaved sequence. Let

$$\mathcal{A}_{\underline{u}} = \begin{bmatrix} u_0 & \cdots & u_{w-1} \\ \vdots & \vdots & \vdots \\ u_{(v-1)w} & \cdots & u_{(v-1)w+w-1} \end{bmatrix} = \begin{bmatrix} u_{0,0} & \cdots & u_{0,w-1} \\ \vdots & \vdots & \vdots \\ u_{v-1,0} & \cdots & u_{v-1,w-1} \end{bmatrix}$$

be the matrix form of $\underline{u}$. Let A_j be the j^{th} column. We observe that the first entry in the sequence $L^\tau(\underline{u})$ is $u_{r,s}$ in $\mathcal{A}_{\underline{u}}$. From the definition of the interleaved sequences, we have $u_{r,v+j} = u_{r+1,j}$ for each j with $v - s \leq j < w$. So T has the following matrix form

$$T = \begin{bmatrix} u_{r,s} & \cdots & u_{r,w-1} & u_{r+1,0} & \cdots & u_{r+1,s-1} \\ u_{r+1,s} & \cdots & u_{r+1,w-1} & u_{r+2,0} & \cdots & u_{r+2,s-1} \\ \vdots & & & & & \\ u_{v-1,s} & \cdots & u_{v-1,w-1} & u_{1,0} & \cdots & u_{1,s-1} \\ \vdots & & & & & \\ u_{r-1,s} & \cdots & u_{r-1,w-1} & u_{r,0} & \cdots & u_{r,s-1} \end{bmatrix}.$$

Therefore, for $0 \leq j < w - s$, we recall

$$T_j = L^r(A_{s+j}) = L^r(L^{e_{s+j}}(\underline{a})) = L^{r+e_{s+j}}(\underline{a}). \tag{5.1}$$

For $w - s \leq j < w$, we have

$$T_j = L^{r+1}(A_{j-(w-s)}) = L^{r+1}(L^{e_{j-(w-s)}}(\underline{a})) = L^{r+1+e_{j-(w-s)}}(\underline{a}). \tag{5.2}$$

For $0 \leq j \leq w - 1$, define

$$e_{j+w} = 1 + e_j. \tag{5.3}$$

Then, the sequence $\underline{e}$ of period w can be expanded to a sequence of period $2w$. For simplicity we still use the symbol $\underline{e}$ for that sequence.

Applying (5.3) for $w - s \leq j \leq w - 1$ we obtain

$$1 + e_{j-(w-s)} = e_{j-(w-s)+w} = e_{s+j}.$$

Substituting it into (5.2), we get that $T_j = L^{r+e_{j+s}}(\underline{a})$. Together with (5.1), the result follows. □

From Proposition 5.2, the following modification of Lemma 1 in [**5**] is immediate.

LEMMA 5.3. *Let $\mathfrak{S}$ be a family of sequences constructed using Algorithm 3.2, and let $\tau = rw + s$ with $0 \leq s < w$ and $0 \leq r < v$. Then, for $\underline{s_k} \in \mathfrak{S} \setminus \{\underline{s_w}\}$, the j^{th} column sequence of $L^\tau(\underline{s_k})$ is given by*

$$L^{r+e_{s+j}}(\underline{a}) + b_{k+s+j}, \quad 0 \leq j < w.$$

Moreover, the j^{th} column sequence of $\underline{s_w}$ is given by $L^{r+e_{s+j}}(\underline{a})$.

REMARK 5.4. Let $\underline{s_h}, \underline{s_k} \in \mathfrak{S}$ be two sequences in the $(v, w)-$interleaved sequence family from Algorithm 3.2. Let $S = (S_0, \ldots, S_{w-1})$ and $T = (T_0, \ldots, T_{w-1})$ be the matrix forms of $\underline{s_h}$ and $L^\tau(\underline{s_k})$, respectively, where $\tau \geq 0$. Proposition 5.1 (2) and Proposition 5.2 imply that the cross correlation between $\underline{s_h}$ and $\underline{s_k}$ can be computed as

$$C_{h,k}(\tau) = \sum_{j=0}^{w-1} < S_j, T_j > .$$

Similarly we have the following modification of Lemma 2 in [**5**].

LEMMA 5.5. *For $0 \le h, k \le w$, suppose that $\underline{s_h}$ and $\underline{s_k}$ are two sequences in $\mathfrak{S}$. If $\tau = rw + s$, $0 \le s < w$, $0 \le r < v$, then the correlation function between $\underline{s_h}$ and $\underline{s_k}$ is*

$$C_{h,k}(\tau) = \begin{cases} \sum_{j=0}^{w-1} (-1)^{b_{h+j} - b_{k+s+j}} C_{\underline{a}}(e_{j+s} - e_j + r), & 0 \le h \le w-1, \\ \sum_{j=0}^{w-1} (-1)^{b_{k+s+j}} C_{\underline{a}}(e_{j+s} - e_j + r), & h = w. \end{cases}$$

PROOF. Let $S = (S_0, \ldots, S_{w-1})$ and $T = (T_0, \ldots, T_{w-1})$ be the matrix forms of $\underline{s_h}$ and $L^\tau(\underline{s_k})$, respectively. According to Remark 5.4,

$$C_{h,k}(\tau) = \sum_{j=0}^{w-1} < S_j, T_j > .$$

First we consider $0 \le h \le w-1$. From Lemma 5.3, for $0 \le j < w$, we have

$$S_j = L^{e_j}(\underline{a}) + b_{k+j}, \qquad T_j = L^{r+e_{s+j}}(\underline{a}) + b_{k+s+j}.$$

Applying Proposition 5.1 (4) and then Proposition 5.1 (3), we get

$$\begin{aligned} < S_j, T_j > &= < L^{e_j}(\underline{a}) + b_{h+j}, L^{r+e_{s+j}}(\underline{a}) + b_{k+s+j} > \\ &= (-1)^{b_{h+j} + b_{k+s+j}} < L^{e_j}(\underline{a}), L^{r+e_{s+j}}(\underline{a}) > \\ &= (-1)^{b_{h+j} - b_{k+s+j}} C_{\underline{a}}(e_{j+s} - e_j + r). \end{aligned}$$

The case $h = w$ can be shown similarly. □

REMARK 5.6. We recall that $\underline{e} = (e_0, \ldots, e_{w-1})$, where $e_{w-1} = \infty$. In order to study $e_{j+s} - e_j$ for $0 \le j, s < w$, we introduce three elements: ∞, ∞_1, and ∞_2, and define $\infty - \infty = \infty$, $k - \infty = \infty_1$ and $\infty - k = \infty_2$ for any integer k.

NOTATION 5.7. Let $d_i = e_{i+1} - e_i$ be in an arithmetic progression for $i = 0, \ldots, w-3$. For $0 \le r < v$, $1 \le s < w$, let $N(r, s)$ be the number of j with $0 \le j < w$ such that $e_{j+s} - e_j + r \equiv 0 \pmod{v}$.

LEMMA 5.8. *For $0 \le r < v$, $1 \le s < w$, let $N(r, s)$ be the number of j with $0 \le j < w$ such that $e_{j+s} - e_j + r \equiv 0 \pmod{v}$, then $N(r, s) \le \lfloor \frac{w}{v} \rfloor + 1$.*

PROOF. For the shift sequence $\underline{e} = (e_0, \ldots, e_{w-1})$, we need $d_0 = e_1 - e_0, d_1 = e_2 - e_1, \ldots, d_{w-2} = e_{w-1} - e_{w-2}$ to be in an arithmetic progression with a constant difference d. So we deduce that $e_i = e_0 + id_0 + \frac{i(i-1)d}{2}$. Since $j + s = w$ gives $e_{j+s} - e_j + r = \infty_2$, we consider the following two cases:

(1) $j + s < w$. We have

$$\begin{aligned} e_{j+s} - e_j + r &= (j+s)d_0 + \frac{(j+s)(j+s-1)d}{2} - jd_0 - \frac{j(j-1)d}{2} + r \\ &= \left(sd_0 + r + \frac{(s^2 - s)d}{2} \right) + sdj. \end{aligned}$$

This is a linear equation modulo v. It has no solution or one solution for j when $j < v$. Thus in the extended $\underline{e}$, there are at most $\lfloor \frac{w}{v} \rfloor + 1$ $j's$ satisfying $e_{j+s} - e_j + r \equiv 0 \pmod{v}$, and $j < w$.

(2) $j < w < j + s$. The above expression changes into

$$\begin{aligned} e_{j+s} - e_j + r &= 1 + e_{(j+s)(\bmod\ w)} - e_j + r \\ &= 1 + (j+s-w)d_0 + \frac{(j+s-w)(j+s-1)d}{2} - jd_0 - \frac{j(j-1)d}{2} + r \\ &= 1 + (s-w)d_0 + r + \frac{(s-w)^2 - (s-w)}{2}d + (s-w)dj. \end{aligned}$$

This equation has at most one solution for $j < v$, and so has at most $\lfloor \frac{w}{v} \rfloor + 1$ solutions when $j < w$. □

We comment that a different proof of the above result is in [**8**]. From Lemma 5.5, we find that the cross correlation of any two sequences in the constructed family is related to $C_{\underline{a}}(e_{j+s} - e_j + r)$. Let $\underline{a}$ be a balanced sequence of period v with $(v-1)/2$ zeros. Then we can denote $C_{\underline{a}}(\infty_1) = C_{\underline{a}}(\infty_2) = -1$ and $C_{\underline{a}}(\infty - \infty + k) = v$. Indeed, the sequence $\underline{a}$ will turn into the zero sequence after shifting it for infinitely many times. Therefore, $C_{\underline{a}}(\infty_1) = \sum_{i=0}^{v-1}(-1)^{a_i - 0} = -1$ since it has $(v-1)/2$ zeros in any period. The same reason leads to $C_{\underline{a}}(\infty_2) = -1$. Similarly, we get $C_{\underline{a}}(\infty - \infty) = \sum_{i=0}^{v-1}(-1)^{0-0} = v$. We comment that these notations are convenient in the case $j + s = w - 1$ or $j = w - 1$, that is, when one of the terms in $e_{j+s} - e_j$ is ∞.

THEOREM 5.9. *Let $\underline{a}$ be a two-level autocorrelation sequence with period v and $\underline{b}$ be a balanced low cross correlation sequence of period w with the maximal absolute value of nontrivial autocorrelation equal to δ_b. The family of sequences $\mathfrak{S}$ generated by Algorithm 3.2 is a $(vw, w+1, \delta_1)$ signal set, where*

$$\delta_1 = \max\left\{\left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)(v+1) + w, \delta_b v\right\}.$$

PROOF. We know that the autocorrelation of $\underline{a}$ is $C_{\underline{a}}(\tau) = \{-1, v\}$.

`Case 1.` $\tau = 0$. It follows $\tau = 0 \cdot w + 0$, that is, $r = s = 0$. By Lemma 5.5 we have

$$C_{h,k}(0) = \begin{cases} \sum_{j=0}^{w-1}(-1)^{b_{h+j} - b_{k+j}} C_{\underline{a}}(0), & 0 \le h \le w-1, \\ \sum_{j=0}^{w-1}(-1)^{b_{k+j}} C_{\underline{a}}(0), & h = w. \end{cases}$$

Since $C_{\underline{a}}(\tau) = \{-1, v\}$, we have

$$C_{\underline{a}}(0) \cdot \sum_{j=0}^{w-1}(-1)^{b_{h+j} - b_{k+j}} = v \cdot \sum_{j=0}^{w-1}(-1)^{b_{h+j} - b_{k+j}} = v \cdot C_{\underline{b}}(h-k).$$

We want to find the nontrivial correlation value. So when $\tau = 0$, the two sequences $\underline{s_h}$, $\underline{s_j}$ should be different. Hence $|C_{h,k}(0)| \le \delta_b v$.
When one of the sequences $\underline{s_h}$ or $\underline{s_k}$ is $\underline{u}$, we have

$$|C_{h,k}(\tau)| = v \cdot \left| \sum_{j=0}^{w-1}(-1)^{b_{j+k}} \right| \le v,$$

because the sequence $\underline{b}$ is balanced.

`Case 2.` $\tau = rw + 0$ and $0 < r < v$.
In this case since $s = 0$ and $r \neq 0$, we have $e_{j+s} - e_j + r = r \pmod v$ and so $N(r, 0) = \{0\}$. Then, for $0 \le h, k < w$, we have

$$C_{h,k}(\tau) = \sum_{j=0}^{w-1} (-1)^{b_{h+j}-b_{k+j}} C_{\underline{a}}(r) = C_{\underline{a}}(r) \cdot C_{\underline{b}}(h-k) = (-1) \cdot C_{\underline{b}}(h-k).$$

Hence $|C_{h,k}(\tau)| \leq w$.

When one of the sequences $\underline{s_h}$ or $\underline{s_k}$ is $\underline{u}$, we have

$$|C_{h,k}(\tau)| = \left| \sum_{j=0}^{w-1} (-1)^{b_{w+j}} C_{\underline{a}}(r) \right| = \left| C_{\underline{a}}(r) \cdot \sum_{j=0}^{w-1} (-1)^{b_j} \right| \leq \left| C_{\underline{a}}(r) \right| = 1.$$

`Case 3.` $\tau = rw + s$ $(0 \leq r < v,\ 0 < s < w)$.
For $0 \leq h, k \leq w$, we have

$$C_{\underline{a}}(e_{j+s} - e_j + r) = \begin{cases} v, & e_{j+s} - e_j + r \equiv 0 \pmod{v}, \\ -1, & e_{j+s} - e_j + r \not\equiv 0 \pmod{v}, \\ -1, & e_{j+s} - e_j + r = \infty_1 \text{ or } \infty_2. \end{cases}$$

We only need to categorize the values of $N(r,s)$ to calculate $C_{h,k}(\tau)$. We consider the following cases:

`Case 3.1:` If $N(r,s) = 0$, there is no j satisfying $e_{j+s} - e_j + r \equiv 0 \pmod{v}$ and so for $0 \leq h, k < w$ and $0 \leq j \leq w-1$, we have $C_{\underline{a}}(e_{j+s} - e_j + r) = -1$. Thus,

$$C_{h,k}(\tau) = (-1) \cdot C_{\underline{b}}(k+s-h).$$

The maximal absolute value of the correlation values is

$$|C_{h,k}(\tau)| \leq \left| C_{\underline{b}}(k+s-h) \right| = w.$$

When one of the sequences $\underline{s_h}$ or $\underline{s_k}$ is $\underline{u}$, the correlation value is

$$\left| C_{\underline{a}}(e_{j+s} - e_j + r) \cdot \sum_{j=0}^{w-1} (-1)^{b_j} \right| \leq 1.$$

`Case 3.2:` If $N(r,s) = 1$, there is one j, say j_0, satisfying $e_{j_0+s} - e_{j_0} + r \equiv 0 \pmod{v}$, then, for $0 \leq h, k < w$, we have

$$\begin{aligned} C_{h,k}(\tau) &= \sum_{j=0}^{q-1} (-1)^{b_{h+j}-b_{k+s+j}} C_{\underline{a}}(e_{j+s} - e_j + r) \\ &= (-1)^{b_{h+j_0}-b_{k+s+j_0}} \cdot C_{\underline{a}}(0) + \sum_{j \neq j_0} (-1)^{b_{h+j}-b_{k+s+j}} \cdot (-1) \\ &= (-1)^{b_{h+j_0}-b_{k+s+j_0}} (v+1) + (-1) \sum_{j=0}^{q-1} (-1)^{b_{h+j}-b_{k+s+j}} \\ &= (-1)^{b_{h+j_0}-b_{k+s+j_0}} (v+1) + (-1) \cdot C_{\underline{b}}(k+s-h) \\ &= (-1) \cdot C_{\underline{b}}(k+s-h) + \{\pm(v+1)\}. \end{aligned}$$

Therefore

$$|C_{h,k}(\tau)| \leq (v+1) + w.$$

When one of the sequences $\underline{s_h}$ or $\underline{s_k}$ is $\underline{u}$, we get

$$\begin{aligned} C_{h,k}(\tau) &= \sum_{j=0}^{w-1}(-1)^{b_{k+s+j}}C_{\underline{a}}(e_{j+s}-e_j+r) \\ &= (-1)^{b_{k+s+j_0}}\cdot C_{\underline{a}}(0)+\sum_{j\neq j_0}(-1)^{b_{k+s+j}}\cdot(-1) \\ &= (-1)^{b_{k+s+j_0}}(v+1)+(-1)\sum_{j=0}^{w-1}(-1)^{b_{k+s+j}}. \end{aligned}$$

Hence,

$$|C_{h,k}(\tau)| \leq (v+1)+1.$$

`Case 3.3:` If $N(r,s)=2$, there are two $j's$, say j_0 and j_1, satisfying $e_{j+s}-e_j+r \equiv 0 \pmod v$. Then, for $0 \leq h,k < w$,

$$\begin{aligned} C_{h,k}(\tau) &= \sum_{j=0}^{w-1}(-1)^{b_{h+j}-b_{k+s+j}}C_{\underline{a}}(e_{j+s}-e_j+r) \\ &= (-1)^{b_{h+j_0}-b_{k+s+j_0}}\cdot C_{\underline{a}}(0)+(-1)^{b_{h+j_1}-b_{k+s+j_1}}\cdot C_{\underline{a}}(0) \\ &\quad +\sum_{j\neq j_0,j_1}(-1)^{b_{h+j}-b_{k+s+j}}\cdot(-1) \\ &= \{\pm(v+1)\}+\{\pm(v+1)\}+(-1)\cdot C_{\underline{b}}(k+s-h). \end{aligned}$$

Therefore,

$$|C_{h,k}(\tau)| \leq 2(v+1)+w.$$

When one of the sequences $\underline{s_h}$ or $\underline{s_k}$ is $\underline{u}$, we obtain

$$\begin{aligned} C_{h,k}(\tau) &= \sum_{j=0}^{w-1}(-1)^{b_{k+s+j}}C_{\underline{a}}(e_{j+s}-e_j+r) \\ &= \{\pm(v+1)\}+\{\pm(v+1)\}+(-1)\sum_{j=0}^{w-1}(-1)^{b_{k+s+j}}. \end{aligned}$$

Thus,

$$|C_{h,k}(\tau)| \leq 2(v+1)+1.$$

`Case 3.4:` As we can see from the previous subcases, the maximum magnitude of the correlation value in our estimations grows as $N(r,s)$ increases. Hence we only give here the estimates for the largest value of $N(r,s)$.

If $N(r,s)=\lfloor \frac{w}{v} \rfloor + 1$, then for $0 \leq h,k < w$, we have

$$C_{h,k}(\tau) = \{\pm(v+1)\}+\cdots+\{\pm(v+1)\}+(-1)\cdot C_{\underline{b}}(k+s-h),$$

where the number of copies of $\{\pm(v+1)\}$ is $\lfloor \frac{w}{v} \rfloor + 1$. Thus

$$|C_{h,k}(\tau)| \leq \left|-\left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)\cdot(v+1)-w\right| = \left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)\cdot(v+1)+w.$$

If one of the sequences $\underline{s_h}$ or $\underline{s_k}$ is $\underline{u}$,

$$|C_{h,k}(\tau)| \leq \left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)\cdot(v+1)+1.$$

Recall that δ_1 denotes the maximum magnitude among all the cross correlation values and nontrivial autocorrelation values of $\mathfrak{S}$. Hence we obtain a $(vw, w+1, \delta_1)$ signal set, where

$$\delta_1 = \max\left\{\left(\left\lfloor\frac{w}{v}\right\rfloor + 1\right)(v+1) + w, \delta_b v\right\}.$$

□

The previous theorem has full generality. We do not require that two sequences $\underline{a}$ and $\underline{b}$ have the same period, nor that the sequence $\underline{b}$ is two-level autocorrelated. In the next theorem we focus on an important case when both two base sequences have two-level autocorrelation (and thus they are balanced as well).

THEOREM 5.10. *If both $\underline{a}$ and $\underline{b}$ are two-level autocorrelation sequences with periods v and w, respectively, then the family of sequences constructed by Algorithm 3.2 is a $(vw, w+1, \delta_2)$ signal set with*

$$\delta_2 = \left(\left\lfloor\frac{w}{v}\right\rfloor + 1\right)(v+1) + 1.$$

PROOF. The proof is similar to Theorem 5.9 but requires further refinements. In particular, in this case $\delta_b = 1$ because sequence $\underline{b}$ is two-level autocorrelated.

- When $k + s - h \equiv 0 \pmod{w}$, the correlaton function

$$C_{\underline{b}}(k+s-h) = \sum_{j=0}^{w-1} (-1)^{b_{k+s+j} - b_{h+j}} = w.$$

It is equivalent to that the sequence $L^{k+s}(\underline{b}) - L^h(\underline{b})$ is the zero sequence. By Lemma 5.5, we have

$$\begin{aligned}
|C_{h,k}(\tau)| &= \left|\sum_{j=0}^{w-1} (-1)^{b_{h+j} - b_{k+s+j}} C_{\underline{a}}(e_{j+s} - e_j + r)\right| \\
&= \left|\sum_{j=0}^{w-1} C_{\underline{a}}(e_{j+s} - e_j + r)\right| \\
&\leq \left(\left\lfloor\frac{w}{v}\right\rfloor + 1\right) \cdot \left|\sum_{j=0}^{v-1} C_{\underline{a}}(e_{j+s} - e_j + r)\right| \\
&\leq \left(\left\lfloor\frac{w}{v}\right\rfloor + 1\right) \cdot v.
\end{aligned}$$

The last inequality holds because there is at most one j such that $e_{j+s} - e_j + r \equiv 0 \pmod{v}$.

- When $k + s - h \not\equiv 0 \pmod{w}$, let $j_0, \ldots, j_{\lfloor\frac{w}{v}\rfloor}$ be the solutions from 0 to $w-1$ such that $e_{j+s} - e_j + r \equiv 0 \pmod{v}$. We observe that this is the case that gives the worst possible cross correlation value. Then the correlaton

function satisfies

$$\begin{aligned}
|C_{h,k}(\tau)| &= \left|\sum_{j=0}^{w-1}(-1)^{b_{h+j}-b_{k+s+j}}C_{\underline{a}}(e_{j+s}-e_j+r)\right| \\
&= \Big|(-1)^{b_{h+j_0}-b_{k+s+j_0}}\cdot C_{\underline{a}}(0)+\cdots+(-1)^{b_{h+j_{\lfloor \frac{w}{v}\rfloor}}-b_{k+s+j_{\lfloor \frac{w}{v}\rfloor}}}\cdot C_{\underline{a}}(0) \\
&\quad + \sum_{j\neq j_0,\ldots,j_{\lfloor \frac{w}{v}\rfloor}}(-1)^{b_{h+j}-b_{k+s+j}}\cdot(-1)\Big| \\
&= \big|\{\pm(v+1)\}+\cdots+\{\pm(v+1)\}+(-1)\cdot C_{\underline{b}}(k+s-h)\big| \\
&\leq \left(\left\lfloor\frac{w}{v}\right\rfloor+1\right)\cdot(v+1)+1.
\end{aligned}$$

Hence, the maximal absolute value of the correlation values is

$$|C_{h,k}(\tau)| \leq \left(\left\lfloor\frac{w}{v}\right\rfloor+1\right)\cdot(v+1)+1.$$

□

We emphasize again that it is more desirable to generate more sequences in a family of sequences and thus we can assume $w \geq v$. This means that we use $\underline{a}$ as the first base sequence and $\underline{b}$ as the second base sequence. In particular, when $v = w$ and the two base sequences are two-level autocorrelated, we recover Gong's result (Theorem 2 in [**5**] or page 364 in [**3**]).

COROLLARY 5.11. When v and w are equal, the family of sequences generated by Algorithm 3.2 is a $(v^2, v+1, 2v+3)$ signal set.

Next we obtain a few results when both base sequences $\underline{a}$ and $\underline{b}$ are Legendre sequences with the period equal to prime number p and q, respectively. We recall that the Legendre sequence $\underline{a}$ of period $p \equiv 3 \pmod 4$ has ideal two-valued autocorrelation $C_{\underline{a}}(\tau) = \{-1, p\}$.

COROLLARY 5.12. Fix a prime number $p \equiv 3 \pmod 4$ and any other prime $q \geq p$. The family of sequences $\mathfrak{S}$ generated by Algorithm 3.2 from two Legendre sequences of periods p and q is a $(pq, q+1, \delta)$ signal set, where

$$\delta = \delta_1 = \left(\left\lfloor\frac{q}{p}\right\rfloor+1\right)\cdot(p+1)+q.$$

Furthermore, when both p and q are congruent to 3 (mod 4) we obtain

$$\delta = \delta_2 = \left(\left\lfloor\frac{q}{p}\right\rfloor+1\right)\cdot(p+1)+1.$$

We remark that Wang and Qi's result is the case when taking two Legendre sequences $\underline{a}$ and $\underline{b}$ with twin prime periods $p \equiv 3 \pmod 4$ and $q = p+2$, respectively.

COROLLARY 5.13. [**8**] Let two Legendre sequences of twin prime periods p and $p+2$, where $p \equiv 3 \pmod 4$ be the base sequences under the construction of the algorithm. The maximum magnitude of nontrivial cross correlation values of this constructed family is $3p+4$.

If Legendre sequence $\underline{a}$ has the prime period $p \equiv 1 \pmod 4$, then $\underline{a}$ is not two-level autocorrelated. In fact, it is three-level correlated. In this case, we slightly modify this Lengedre sequence so that we have a two-level autocorrelation sequence $\underline{a'}$.

LEMMA 5.14. *Let $\underline{a}$ be a Legendre sequence with prime period $p \equiv 1 \pmod 4$. If we let the entries $a'_i = -\infty$ with $i \equiv 0 \pmod p$ and $a'_i = a_i$ with $i \not\equiv 0 \pmod p$, then the modified Legendre sequence $\underline{a'}$ has two-valued autocorrelation.*

PROOF. The proof is on page 294 in [**6**]. □

Now we estimate the maximal cross correlation of the interleaved construction from $\underline{a}$ and $\underline{b}$ by using the maximal cross correlation of the interleaved construction from $\underline{a'}$ and $\underline{b}$.

THEOREM 5.15. *Fix a prime number $p \equiv 1 \pmod 4$ and any other prime $q \geq p$. The family of sequences $\mathfrak{S}$ generated by Algorithm 3.2 from two Legendre sequences of periods p and q is a $(pq, q+1, \delta_3)$ family, where $\delta_3 = \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right) \cdot (p+1) + 3q - 2$.*

PROOF. Fix a prime $p \equiv 1 \pmod 4$, we use the modified Legendre sequence $\underline{a'} = (-\infty, a_1, \ldots, a_{p-1})$ as the first base sequence in Algorithm 3.2. Then by Theorem 5.9, the family of sequence $\mathfrak{S}'$ constructed from $\underline{a'}$ and $\underline{b}$ has the maximal correlation value

$$|C_{h,k}(\tau)'| \leq \delta_1 = \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right) \cdot (p+1) + q.$$

For each sequence $\underline{s_j}' \in \mathfrak{S}'$, we have $\underline{s_j}' = \underline{u}' + L^j(\underline{b})$ and every column of the matrix form of the interleaved sequence $\underline{u}'$ contains a $-\infty$. Therefore, there are $q-1$ copies of $-\infty$'s in every sequence $\underline{s_j}' \in \mathfrak{S}'$ for $j = 0, \ldots, q$. If sequence $\underline{s_j}$ in the family of sequences is constructed by Algorithm 3.2 from ordinary Legendre sequence $\underline{a}$ and $\underline{b}$, then the difference between $\underline{s_j}$ and the corresponding $\underline{s_j}'$ happens exactly at these entries of $-\infty$ in $\underline{s_j}'$. Then the correlation function of any two sequences $\underline{s_j} = (s_{j0}, s_{j1}, \ldots, s_{j(q-1)})$, $\underline{s_k} = (s_{k0}, \ldots, s_{k(q-1)})$ in the family $\mathfrak{S}$ constructed from the ordinary Legendre sequence $\underline{a}$ and $\underline{b}$ is

$$\begin{aligned} |C_{h,k}(\tau)| &\leq |C_{h,k}(\tau)'| + 2(q-1) \\ &\leq \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right) \cdot (p+1) + q + 2(q-1) \\ &= \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right) \cdot (p+1) + 3q - 2. \end{aligned}$$

□

6. Conclusions

In this paper we study interleaved constructions of low cross correlation sequences including their balance and cross correlation properties. In particular, we generalize Gong's results of interleaved sequences of two-level autocorrelation sequences of the same period to the case where the periods are distinct. Moreover, we study interleaved sequences constructed from two Legendre sequences of periods p and q, where p and q are prime numbers. We give the balance and cross correlation properties as well. For further work, it would be interesting to have a study of the linear complexity, merit factors, and aperiodic correlation of these constructions.

Acknowledgements

We thank the referee for very helpful suggestions which lead to a significant improvement of the results.

References

[1] C. Ding, T. Helleseth and W. Shan, "On the linear complexity of Legendre sequences", IEEE Trans. Inform. Theory, vol. 44, 1276-1278, 1998.
[2] S. W. Golomb, Shift Register Sequences, Aegean Park Press, 1982.
[3] S. W. Golomb and G. Gong, Signal Design for Good Correlation, Cambridge University Press, 2005.
[4] G. Gong, "Theory and applications of q-ary interleaved sequences", IEEE Trans. Inform. Theory, vol. 41, 400-411, 1995.
[5] G. Gong, "New design for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ case", IEEE Trans. Inform. Theory, vol. 48, 2847-2867, 2002.
[6] M.R. Schroeder, "Number Theory in Science and Communication: with Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity", Third Edition, Springer, Berlin, 1997.
[7] V. M. Sidelnikov, "On mutual correlation of sequences", Sov. Math. Doklady, vol. 12, 197-201, 1971.
[8] J.-S. Wang and W.-F. Qi, "A new class of binary sequence family with low correlation and large linear complexity", Proceeding of IWSDA'07, IEEE, 2007.
[9] L. R. Welch, "Lower bounds on the maximum cross correlation of signals", IEEE Trans. Inform. Theory, vol. 20, 397-399, 1974.

School of Mathematics & Statistics, Carleton University, Ottawa, K1S 5B6, Canada
E-mail address: jhe2@connect.carleton.ca

School of Mathematics & Statistics, Carleton University, Ottawa, K1S 5B6, Canada
E-mail address: daniel@math.carleton.ca

School of Mathematics & Statistics, Carleton University, Ottawa, K1S 5B6, Canada
E-mail address: wang@math.carleton.ca