

The Array Structure of Modified Jacobi Sequences

Shenghua Li¹, Lianfei Luo¹ & Hannuo Zhao¹

¹ Faculty of Mathematics and Statistics, Hubei University, Wuhan, P. R. China

Correspondence: Shenghua Li, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, P. R. China. E-mail: lsh@hubu.edu.cn

Received: January 7, 2014 Accepted: February 4, 2014 Online Published: February 24, 2014

doi:10.5539/jmr.v6n1p100 URL: <http://dx.doi.org/10.5539/jmr.v6n1p100>

Abstract

It is known that the out-of-phase autocorrelation values of modified Jacobi sequences of period pq , p, q prime, are depend only on the difference between p and q . In this paper, the array structure of modified Jacobi sequences is studied. Based on the structure, their autocorrelation functions are computed clearly, and some modifications of modified Jacobi sequences can be obtained.

Keywords: array form, autocorrelation, Legendre sequence, modified Jacobi sequence

MR Subject Classification: 11T71, 94A60, 94A55

1. Introduction

Binary sequences with good autocorrelation have important applications in communications and cryptology (see Golomb & Gong, 2005). The ideal 2-level autocorrelation sequences have been studied since the 1960s, which only have out-of-phase autocorrelation of -1 . The interleaved structure of sequences with composite period is introduced in (Gong, 1995). Based on the structure, it is known that the sequence is determined by two sequences, the base sequence and the shift sequence. Furthermore, some new sequences with good correlation can be constructed by this structure (Gong, 2002). Most of the ideal 2-level autocorrelation sequences of composite period, such as m sequences, GMW sequences, and generalized GMW sequences, have the interleaved structure. Twin prime sequences are the special modified Jacobi sequences and they have ideal 2-level autocorrelation, but do not have the interleaved structure.

For the modified Jacobi sequences (Calabro & Wolf, 1968) with period pq , p, q prime, it is very interesting that the out-of-phase autocorrelation values of them are dependent only on the difference between p and q . In recent years, some modifications of modified Jacobi sequences (Brandstätter, Pirsic, & Winterhof, 2011; Li et al., 2007; Su & Winterhof, 2010; Xiong & Hall, 2011) have been studied, and similar results are obtained by the number theory approach. In Green and Green (2000), the diagonal structure of modified Jacobi sequences is studied. The way to yield the array is to start at the top left-hand corner of the array with the first digit of the sequence and then to place subsequent digits down the diagonal. There, the first row (column) is regarded as the next of the last row (column). In this paper, we investigated another array structure of modified Jacobi sequences, which is rearranged row by row and from left to right within a row. We find that modified Jacobi sequences have interleaved-like structure. Now the sequence is determined by three sequences, two base sequences and one shift sequence. By the structure, the relation between the Jacobi sequence and modified Jacobi sequence is clearly exposed, and the autocorrelation of modified Jacobi sequences can be obtained easily. Furthermore, some modifications of the modified Jacobi sequence can be constructed.

This paper is organized as follows. Section 2 gives some basic concepts and some known results which will be employed throughout this paper. In Section 3, the array structure of modified Jacobi sequences is investigated. In Section 4, the autocorrelation of the modified Jacobi sequence is computed based on the array structure. Discussion and concluding remarks are given in Section 5.

2. Preliminaries

In this section, we introduce some preliminaries which will be used throughout the paper. For more details, the reader is referred to (Cusick, Ding, & Renvall, 1998; Golomb & Gong, 2005).

2.1 Sequences and Crosscorrelation Function

Let $\mathbb{Z}_m$ be a ring of integers modulo m , $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$, and $\mathbb{F}_2 = GF(2)$, the finite field with two elements 0 and 1. For a binary sequence $\mathbf{a} = \{a_i\}$, $a_i \in \mathbb{F}_2$ with period N , $\bar{\mathbf{a}}$ is the complement of $\mathbf{a}$, i.e., $\bar{\mathbf{a}} = \{a_i + 1\}$; $\mathbf{a}^*$ is the companion of $\mathbf{a}$, and defined by $a_0^* = a_0$, $a_i^* = a_i + 1$ for $1 \leq i < N$. For a positive integer r , the r -decimation of $\mathbf{a}$ denoted by $D^r(\mathbf{a})$ is defined as $\{a_{ri}\}$. $L^r(\mathbf{a})$, the left r -shift of $\mathbf{a}$, is defined as $\{a_{i+r}\}$. We use $\mathbf{0}$ for the all zero sequence, and $\mathbf{1}$ for the all one sequence, respectively.

The crosscorrelation of two binary sequences $\mathbf{u}$ and $\mathbf{v}$ with period N is defined as

$$C_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{i=0}^{N-1} (-1)^{u_i + v_{i+\tau}}, \quad \tau = 0, 1, \dots, N-1. \quad (1)$$

If $\mathbf{v} = \mathbf{u}$, then the crosscorrelation function becomes the autocorrelation function, and is denoted by $C_{\mathbf{u}}(\tau)$. It is clear that $C_{\mathbf{u}}(0) = N$. If the out-of-phase autocorrelation value is -1 for odd N or 0 for even N respectively, then the sequence is said to have the ideal 2-level autocorrelation function. The correlation function has following properties:

- 1) $C_{\bar{\mathbf{u}}}(\tau) = C_{\mathbf{u}}(\tau)$;
- 2) $C_{\mathbf{u},\mathbf{v}}(\tau) = C_{\mathbf{v},\mathbf{u}}(-\tau)$;
- 3) $C_{\mathbf{u},\bar{\mathbf{v}}}(\tau) = -C_{\mathbf{u},\mathbf{v}}(\tau)$;
- 4) $C_{L^k(\mathbf{u}), L^j(\mathbf{v})}(\tau) = C_{\mathbf{u},\mathbf{v}}(\tau + j - k)$, $0 \leq j, k < N$.

From the properties above, we have

Lemma 1 With the notation introduced above, suppose the period of $\mathbf{a}$ is N , then

$$C_{\mathbf{a}^*}(\tau) = \begin{cases} N, & \tau = 0, \\ -2[(-1)^{a_0+a_\tau} + (-1)^{a_0+a_{-\tau}}] + C_{\mathbf{a}}(\tau), & \tau \neq 0, \end{cases} \quad (2)$$

$$C_{\mathbf{a},\mathbf{a}^*}(\tau) = \begin{cases} 2 - N, & \tau = 0, \\ 2(-1)^{a_0+a_{-\tau}} - C_{\mathbf{a}}(\tau), & \tau \neq 0. \end{cases} \quad (3)$$

Proof. From the definition of $\mathbf{a}^*$, it is clearly right for the case $\tau = 0$. When $\tau \neq 0$, we only compute $C_{\mathbf{a}^*}(\tau)$, and $C_{\mathbf{a},\mathbf{a}^*}(\tau)$ can be computed similarly.

$$\begin{aligned} C_{\mathbf{a}^*}(\tau) &= \sum_{i=0}^{N-1} (-1)^{a_i^* + a_{i+\tau}^*} \\ &= (-1)^{a_0+a_\tau+1} + (-1)^{a_{-\tau}+a_0+1} + \sum_{i=0}^{N-1} (-1)^{a_i + a_{i+\tau}} - (-1)^{a_0+a_\tau} - (-1)^{a_{-\tau}+a_0}. \end{aligned}$$

Thus, $C_{\mathbf{a}^*}(\tau) = -2[(-1)^{a_0+a_\tau} + (-1)^{a_0+a_{-\tau}}] + C_{\mathbf{a}}(\tau)$ for $\tau \neq 0$. □

2.2 Cyclotomic Classes and Cyclotomic Numbers

For a prime p , let $D_0 = \{x^2 | x \in \mathbb{Z}_p^*\}$, $D_1 = \mathbb{Z}_p^* \setminus D_0$, be the sets of quadratic residues and quadratic nonresidues modulo p , respectively. They are also called the cyclotomic classes of order two. The cyclotomic numbers of order two are defined to be $(i, j) = |(D_i + 1) \cap D_j|$, $i, j \in \{0, 1\}$. We need the following results on cyclotomic classes and cyclotomic numbers of order two.

Lemma 2 (Cusick, Ding, & Renvall, 1998) *Let p be an odd prime, the cyclotomic classes of order two have the following properties:*

- 1) $|D_0| = |D_1| = (p-1)/2$,
- 2) If $w \in D_0$, then $wD_0 = D_0$, $wD_1 = D_1$; If $w \in D_1$, then $wD_0 = D_1$, $wD_1 = D_0$,
- 3) $-1 \in D_0$ if and only if $p \equiv 1 \pmod{4}$.

Lemma 3 (Cusick, Ding, & Renvall, 1998) *Let p be an odd prime, the cyclotomic numbers of order two are given by*

- 1) $(0, 0) = (p-5)/4$, $(0, 1) = (1, 0) = (1, 1) = (p-1)/4$ if $p \equiv 1 \pmod{4}$,

2) $(0, 0) = (1, 0) = (1, 1) = (p - 3)/4$, $(0, 1) = (p + 1)/4$ if $p \equiv 3 \pmod{4}$.

Let $C_0 = D_0 \cup \{0\}$, $C_1 = D_1$, $d(i, j; w) = |C_i \cap (C_j - w)|$, $i, j = 0, 1$, $w \in \mathbb{Z}_p$. The numbers $d(i, j; w)$'s are often used to determine the correlation of sequences which are associated with cyclotomic classes. From the lemma above, we have

Corollary 1 Let p be an odd prime. For any $w, w \in \mathbb{Z}_p^*$, $d(i, j; w)$ are given by

1) If $p \equiv 3 \pmod{4}$, then

$$d(0, 0; w) = (p + 1)/4, \quad d(1, 1; w) = (p - 3)/4, \quad d(0, 1; w) = d(1, 0; w) = (p + 1)/4.$$

2) If $p \equiv 1 \pmod{4}$, then

$$d(0, 0; w) = \begin{cases} (p + 3)/4, & w \in D_0, \\ (p - 1)/4, & w \in D_1, \end{cases} \quad d(1, 1; w) = \begin{cases} (p - 1)/4, & w \in D_0, \\ (p - 5)/4, & w \in D_1, \end{cases}$$

$$d(0, 1; w) = d(1, 0; w) = \begin{cases} (p - 1)/4, & w \in D_0, \\ (p + 3)/4, & w \in D_1. \end{cases}$$

2.3 The Legendre Sequence and Modified Jacobi Sequence

The Legendre sequence $\mathbf{a} = \{a_i\}$ with period p is defined by

$$a_i = \begin{cases} 0, & \text{if } i = 0, \\ 0, & \text{if } i \in D_0, \\ 1, & \text{if } i \in D_1, \end{cases} \quad (4)$$

or its complement, companion, and the companion of its complement. Namely, there are four types of Legendre sequences: $\mathbf{a}$, $\bar{\mathbf{a}}$, $\mathbf{a}^*$ and $\bar{\mathbf{a}}^*$.

From 2) of Lemma 2, the decimation of a Legendre sequence has the following property.

Lemma 4 (Cusick, Ding, & Renvall, 1998) *The r -decimation of a Legendre sequence $\mathbf{a}$ is also a Legendre sequence. Furthermore, $D^r(\mathbf{a}) = \mathbf{a}$ for $r \in D_0$ and $D^r(\mathbf{a}) = \mathbf{a}^*$ for $r \in D_1$.*

The autocorrelation of the Legendre sequence is well-known (Golomb & Gong, 2005). From Lemma 1, we can determine the autocorrelation of its companion and the crosscorrelation between them as follows, which will be used later.

Theorem 1 Let $\mathbf{a}$ be the Legendre sequence of period p defined by (4). Then

1) if $p \equiv 3 \pmod{4}$,

$$C_{\mathbf{a}}(\tau) = C_{\mathbf{a}^*}(\tau) = \begin{cases} p, & \tau = 0, \\ -1, & \text{otherwise,} \end{cases} \quad C_{\mathbf{a}, \mathbf{a}^*}(\tau) = \begin{cases} 2 - p, & \tau = 0, \\ -1, & \tau \in D_0, \\ 3, & \tau \in D_1. \end{cases}$$

2) if $p \equiv 1 \pmod{4}$,

$$C_{\mathbf{a}}(\tau) = \begin{cases} p, & \tau = 0, \\ 1, & \tau \in D_0, \\ -3, & \tau \in D_1, \end{cases} \quad C_{\mathbf{a}^*}(\tau) = \begin{cases} p, & \tau = 0, \\ -3, & \tau \in D_0, \\ 1, & \tau \in D_1, \end{cases} \quad C_{\mathbf{a}, \mathbf{a}^*}(\tau) = \begin{cases} 2 - p, & \tau = 0, \\ 1, & \text{otherwise.} \end{cases}$$

Note that if $\mathbf{a}$ is one of the other three types, the result is similar.

For two primes p and q , the Jacobi sequence (Calabro & Wolf, 1968) is defined as the sum of two Legendre sequences associated with p and q respectively. The out-of-phase autocorrelation values of Jacobi sequences contain the factors p and q , and do not have good autocorrelation. However, modified Jacobi sequences can improve this situation and the out-of-phase autocorrelation values are dependent only on the difference between p and q . When the difference is 2, the sequence has the ideal 2-level autocorrelation function, and is called as a twin primes sequence.

Definition 1 (Calabro & Wolf, 1968) Let $\mathbf{a}$ and $\mathbf{b}$ be the Legendre sequences associated with two odd primes p and q , respectively. The modified Jacobi sequence $\mathbf{s} = \{s_i\}$ of period pq is defined as

$$s_i = \begin{cases} a_i + b_i, & \gcd(i, pq) = 1, \\ 0, & i \equiv 0 \pmod{q}, \\ 1, & \text{otherwise.} \end{cases} \quad (5)$$

When the greatest common divisor of p and q is 2, Ding constructed the generalized cyclotomic sequence of order two in (Ding, 1998), which could also be expressed as (5).

Example 1 Let $p = 5, q = 7$, the Legendre sequences $\mathbf{a} = \{00110\}$ and $\mathbf{b} = \{0001011\}$. Thus, a modified Jacobi sequence of period 35 is given by

$$\mathbf{s} = \{00100110101000010011101111100011101\}.$$

Theorem 2 (Calabro & Wolf, 1968) The autocorrelation of the modified Jacobi sequence $\mathbf{s}$ in Definition 1 is given by

1) If p is congruent to q modulo 4,

$$C_s(\tau) = \begin{cases} pq, & 1 \text{ time,} \\ p - q + 1, & q - 1 \text{ times,} \\ q - p - 3, & p - 1 \text{ times,} \\ 1, & (p - 1)(q - 1)/2 \text{ times,} \\ -3, & (p - 1)(q - 1)/2 \text{ times.} \end{cases} \quad (6)$$

2) If p is not congruent to q modulo 4,

$$C_s(\tau) = \begin{cases} pq, & 1 \text{ time,} \\ p - q + 1, & q - 1 \text{ times,} \\ q - p - 3, & p - 1 \text{ times,} \\ -1, & (p - 1)(q - 1) \text{ times.} \end{cases} \quad (7)$$

3. The Interleaved-like Structure of the Modified Jacobi Sequence

In this section, we will study the array structure of modified Jacobi sequences. We arrange the modified Jacobi sequence $\mathbf{s}$ of period pq as a $p \times q$ array form, which is row by row and from left to right within a row. Thus, the modified Jacobi sequence of period 35 given by Example 1 has the following form:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \quad (8)$$

The array form of a modified Jacobi sequence has the following

Theorem 3 With the same notation of Definition 1, let $\mathbf{M}$ be the $p \times q$ array form of $\mathbf{s}$. Let $\mathbf{v} = D^q(\mathbf{a})$, $\mathbf{u}$ be defined as $u_0 = 1$, $u_i = v_i$ for $i \neq 0$. Then the j th column of $\mathbf{M}$ is given by

$$M_j = \begin{cases} \mathbf{0}, & j = 0, \\ L^{e_j}(\mathbf{u}), & b_j = 0 \text{ and } j \neq 0, \\ L^{e_j}(\mathbf{u}^*), & b_j = 1, \end{cases}$$

where $e_j = q^{-1} \times j \pmod{p}$ for $j \neq 0$.

Proof. It is obvious that $M_0 = \mathbf{0}$ from (5).

For $j \neq 0$, we first investigate the array form $\mathbf{N}$ of the Jacobi sequence $\mathbf{t} = \mathbf{a} + \mathbf{b}$. For any k , $0 \leq k < pq$, let $k = iq + j$, $0 \leq i < p$, $0 \leq j < q$. Then

$$t_{iq+j} = a_{iq+j} + b_{iq+j} = a_{q(i+q^{-1}j)} + b_j.$$

Let $\mathbf{v} = D^q(\mathbf{a})$, $e_j = q^{-1} \times j \pmod{p}$. Thus, the j th column of $\mathbf{N}$, $N_j = L^{e_j}(\mathbf{v})$ for $b_j = 0$, and $N_j = \overline{L^{e_j}(\mathbf{v})}$ otherwise.

Let $N_j = \{N_{j,0}, N_{j,1}, \dots, N_{j,p-1}\}$. Note that

$$N_{j,-q^{-1} \times j} = v_0 + b_j$$

and

$$(-q^{-1} \times j) \pmod{p} \times q + j \equiv 0 \pmod{p}.$$

From (5), for each $j \neq 0$, the l th element of M_j must be 1 if $l = (-q^{-1} \times j) \pmod{p}$, and is equal to $N_{j,l}$ otherwise. Define $\mathbf{u}$ as $u_0 = 1$, $u_i = v_i$ for $i \neq 0$. Note that $\mathbf{u}^* = \bar{\mathbf{v}}$. Therefore, M_j is equal to $L^{e_j}(\mathbf{u})$ for $b_j = 0$, and $L^{e_j}(\mathbf{u}^*)$ for $b_j = 1$, respectively. $\square$

We make a convention that $e_i = \infty$ if the i th column of the array form is $\mathbf{0}$.

Example 2 Let $\mathbf{s}$ be the modified Jacobi sequence of period 35 in Example 1. It is easy to see that $7 \pmod{5} = 2$, $\mathbf{v} = D^2(\mathbf{a}) = \{01001\}$, and so $\mathbf{u} = \{11001\}$ and $\mathbf{u}^* = \{10110\}$. One can check that $\mathbf{e} = (\infty, 3, 1, 4, 2, 0, 3)$ by the array form (8), where $e_j = 7^{-1} \times j \pmod{5} = 3j \pmod{5}$ for $j \neq 0$.

The array form of the interleaved sequence introduced by Gong is determined by the base sequence and the shift sequence completely. However, the array form in Theorem 3 is associated with three sequences. In the following, we give the definition of the interleaved-like sequence.

Definition 2 Let $\mathbf{u}_1$ and $\mathbf{u}_2$ be two binary sequences of period m , and $\mathbf{l}$ be a binary sequence of period n . Let $\mathbf{e} = \{e_0, \dots, e_{n-1}\}$, $e_j \in \mathbb{Z}_m \cup \{\infty\}$. If a binary sequence $\mathbf{s}$ of period mn can be arranged as an $m \times n$ array form $\mathbf{M}$, and the j th column of $\mathbf{M}$, M_j has the following form

$$M_j = \begin{cases} \mathbf{0}, & e_j = \infty, \\ L^{e_j}(\mathbf{u}_1), & l_j = 0 \text{ and } e_j \neq \infty, \\ L^{e_j}(\mathbf{u}_2), & l_j = 1 \text{ and } e_j \neq \infty, \end{cases}$$

then we say that $\mathbf{s}$ is an interleaved-like binary sequence with respect to $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{l}$ and $\mathbf{e}$. And the array form of $\mathbf{s}$ is denoted by $M(\mathbf{u}_1, \mathbf{u}_2, \mathbf{l}, \mathbf{e})$. The sequences $\mathbf{u}_1$ and $\mathbf{u}_2$ are called the base sequences of $\mathbf{s}$, $\mathbf{l}$ and $\mathbf{e}$ are called the label sequence and shift sequence of $\mathbf{s}$, respectively.

Remark 1 Let $\mathbf{u}$ be an interleaved sequence with base sequence $\mathbf{a}$ and shift sequence $\mathbf{e}$. Then, $\mathbf{u}$ can be viewed as the interleaved-like sequence with the array form $M(\mathbf{a}, \mathbf{a}, \mathbf{0}, \mathbf{e})$. The signal set $\{s_k\}$ in (Gong, 2002) was defined as $s_k = \mathbf{u} + L^k(\mathbf{b})$. Thus, s_k is an interleaved-like sequence with the array form $M(\mathbf{a}, \bar{\mathbf{a}}, L^k(\mathbf{b}), \mathbf{e})$.

To determine the autocorrelation of an interleaved-like sequence $\mathbf{s}$, we need to consider the array form of $L^\tau(\mathbf{s})$. First, the shift sequence $\mathbf{e}$ is extended to $\{e_0, \dots, e_{mn-1}\}$ as follows. For $k = in + j$ with $0 \leq i < m$, $0 \leq j < n$,

$$e_{in+j} = \begin{cases} e_j + i \in \mathbb{Z}_m, & \text{if } e_j \neq \infty, \\ \infty, & \text{otherwise.} \end{cases}$$

Theorem 4 With the same notation of Definition 2. For $\tau = vn + r$, $0 \leq v < m$, $0 \leq r < n$, the array form of $L^\tau(\mathbf{s})$ is given by $M(\mathbf{u}_1, \mathbf{u}_2, L^r(\mathbf{l}), \mathbf{e}')$, where the new shift sequence $\mathbf{e}' = \{e'_0, \dots, e'_{n-1}\}$ is given by

$$e'_j = \begin{cases} e_{j+r} + v \pmod{m}, & \text{if } e_{j+r} \neq \infty, \\ \infty, & \text{otherwise.} \end{cases} \quad (9)$$

Proof. Let $\mathbf{t} = L^\tau(\mathbf{s})$. Let $\mathbf{A} = (A_0, \dots, A_{n-1})$ and $\mathbf{T} = (T_0, \dots, T_{n-1})$ be the array forms of $\mathbf{s}$ and $\mathbf{t}$, respectively. For any k , $0 \leq k < pq$, let $k = in + j$, $0 \leq i < m$, $0 \leq j < n$. Then, $t_k = s_{k+\tau} = s_{(i+v)n+r+j}$. Therefore,

$$T_j = \begin{cases} L^v(A_{j+r}), & 0 \leq j < n-r, A_{j+r} \neq \mathbf{0} \\ L^{v+1}(A_{j+r-n}), & n-r \leq j < n, A_{j+r-n} \neq \mathbf{0}. \end{cases}$$

Combining with the extension of $\mathbf{e}$, we know that the base sequences of $L^\tau(\mathbf{s})$ are the same as those of $\mathbf{s}$, the label sequence is $L^\tau(\mathbf{I})$, and the shift sequence $\mathbf{e}'$ is given by (9). $\square$

The autocorrelation of an interleaved-like sequence $\mathbf{s}$ can be computed by the array forms of $\mathbf{s}$ and $L^\tau(\mathbf{s})$, which are associated with the autocorrelations of the base sequences, the crosscorrelation between the base sequences, and the difference between the shift sequences of $L^\tau(\mathbf{s})$ and $\mathbf{s}$. From Theorem 3, the modified Jacobi sequence is a special interleaved-like binary sequence. Since the elements of the shift sequence are linear with the column number, the following is obtained from (9).

Theorem 5 With the same notation of Theorem 3. For $\tau = vq + r$, $0 \leq v < p$, $0 \leq r < q$, let $\mathbf{e}'$ be the shift sequence of $L^\tau(\mathbf{s})$. Then,

$$e'_j - e_j \equiv v + q^{-1}r \pmod{p},$$

for $e_j \neq \infty$ and $e'_j \neq \infty$.

4. The Autocorrelation of the Modified Jacobi Sequence

In this section, we determine the autocorrelation of the modified Jacobi sequence $\mathbf{s}$ by its array structure.

The autocorrelation $C_s(\tau)$ will be computed column by column from the array forms of $\mathbf{s}$ and $L^\tau(\mathbf{s})$. Let $\mathbf{A} = (A_0, \dots, A_{q-1})$ and $\mathbf{B} = (B_0, \dots, B_{q-1})$ be the array forms of them, respectively. Note that the base sequences are $\mathbf{u}$ and $\mathbf{u}^*$, and they are also Legendre sequences. The correlations of the base sequences are given by Theorem 1. Let $\tau = vq + r$, $0 \leq v < p$, $0 \leq r < q$, $\delta = v + q^{-1}r \pmod{p}$, the autocorrelation of $\mathbf{s}$ can be computed as

$$C_s(\tau) = \sum_{j=0}^{q-1} \langle A_j, B_j \rangle,$$

$$\text{where } \langle A_j, B_j \rangle = \sum_{i=0}^{p-1} (-1)^{A_{i,j} + B_{i,j}}.$$

If $r = 0$, $C_s(\tau) = p + (C_{\mathbf{u}}(\delta) + C_{\mathbf{u}^*}(\delta)) \times \frac{q-1}{2}$. Thus, $C_s(\tau) = pq$ for $\delta = 0$, or $p - q + 1$ otherwise.

If $r \neq 0$, let $\mathbf{A}' = (A'_0, \dots, A'_{q-1})$ be defined by $A'_0 = \mathbf{u}$, $A'_j = A_j$ for $j \neq 0$. Assume that the sequence respected to $\mathbf{A}'$ is denoted by $\mathbf{s}'$ and $\mathbf{B}' = (B'_0, \dots, B'_{q-1})$ is the array form of $L^\tau(\mathbf{s}')$. The autocorrelation $C_s(\tau)$ can be rewritten as

$$\begin{aligned} C_s(\tau) &= \sum_{j=0}^{q-1} \langle A'_j, B'_j \rangle - (\langle A'_0, B'_0 \rangle + \langle A'_{-r}, B'_{-r} \rangle) + (\langle \mathbf{0}, B_0 \rangle + \langle A_{-r}, \mathbf{0} \rangle) \\ &= C_{s'}(\tau) - (\langle A'_0, B'_0 \rangle + \langle A'_{-r}, B'_{-r} \rangle) - 2, \end{aligned}$$

where the last identity follows from the balance of the Legendre sequence. Let $\Delta(\tau) = \langle A'_0, B'_0 \rangle + \langle A'_{-r}, B'_{-r} \rangle$, then

$$C_s(\tau) = C_{s'}(\tau) - \Delta(\tau) - 2. \quad (10)$$

Note that $\mathbf{s}'$ is an interleaved-like sequence, too. The first element of the shift sequence is 0, and the other elements are not changed. Thus, the difference between the shift sequences of $L^\tau(\mathbf{s}')$ and $\mathbf{s}'$ is δ for each $0 \leq j < q$. On the other hand, the base sequences and the label sequence are not changed. Then, the term $\langle A'_j, B'_j \rangle$ is associated with the autocorrelation of $\mathbf{u}$, or the autocorrelation of $\mathbf{u}^*$, or the crosscorrelation of $\mathbf{u}$ and $\mathbf{u}^*$. These correlations are associated with the cyclotomic classes of p , and the number of each type of correlation depends on the cyclotomic numbers of q . For clarity, the cyclotomic numbers and cyclotomic classes are denoted by $d_q(i, j; w)$ and $D_{p,i}$, respectively. In detail, $C_{s'}(\tau)$ is computed as follows

$$\begin{aligned} C_{s'}(\tau) &= d_q(0, 0; r) \times C_{\mathbf{u}}(\delta) + d_q(1, 1; r) \times C_{\mathbf{u}^*}(\delta) + d_q(0, 1; r) \times C_{\mathbf{u}, \mathbf{u}^*}(\delta) + d_q(1, 0; r) \times C_{\mathbf{u}^*, \mathbf{u}}(\delta) \\ &= d_q(0, 0; r) \times C_{\mathbf{u}}(\delta) + d_q(1, 1; r) \times C_{\mathbf{u}^*}(\delta) + d_q(0, 1; r) \times (C_{\mathbf{u}, \mathbf{u}^*}(\delta) + C_{\mathbf{u}^*, \mathbf{u}}(-\delta)), \end{aligned}$$

where the last identity follows from $d_q(0, 1; r) = d_q(1, 0; r)$.

If $\delta = 0$,

$$C_{s'}(\tau) = p(d_q(0, 0; r) + d_q(1, 1; r)) + 2(2 - p)d_q(0, 1; r). \quad (11)$$

If $\delta \neq 0$, by Theorem 1, we have

$$C_{s'}(\tau) = -d_q(0, 0; r) - d_q(1, 1; r) + 2d_q(0, 1; r), \quad (12)$$

for $p \equiv 3 \pmod{4}$, and

$$C_{s'}(\tau) = \begin{cases} d_q(0, 0; r) - 3d_q(1, 1; r) + 2d_q(0, 1; r), & \text{if } \delta \in D_{p,0}, \\ -3d_q(0, 0; r) + d_q(1, 1; r) + 2d_q(0, 1; r), & \text{if } \delta \in D_{p,1}, \end{cases} \quad (13)$$

for $p \equiv 1 \pmod{4}$.

Now, we can determine the autocorrelation of the modified Jacobi sequence $\mathbf{s}$ from Corollary 1, and thus give an alternative proof of Theorem 2.

Proof of Theorem 2. We only need to compute $C_s(\tau)$ when $r \neq 0$ in view of the values of p, q modulo 4. Here we only compute $C_s(\tau)$ when $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$. For the other three cases, it can be computed similarly.

For this case, by Corollary 1, (11) and (12), we get

$$C_{s'}(\tau) = \begin{cases} q - p + 1, & \delta = 0, \\ 1, & \text{otherwise.} \end{cases}$$

Next, we consider $\Delta(\tau)$. There are two subcases.

1) If $r \in D_{q,0}$, then $-r \in D_{q,1}$, and so

$$\Delta(\tau) = C_{\mathbf{u}}(\delta) + C_{\mathbf{u}^*, \mathbf{u}}(\delta) = C_{\mathbf{u}}(\delta) + C_{\mathbf{u}, \mathbf{u}^*}(-\delta).$$

From Theorem 1, $\Delta(\tau) = -2$ for $\delta \in D_{p,1}$, or 2 otherwise.

2) If $r \in D_{q,1}$, then $-r \in D_{q,0}$, and so

$$\Delta(\tau) = C_{\mathbf{u}, \mathbf{u}^*}(\delta) + C_{\mathbf{u}}(\delta).$$

Thus, from Theorem 1, $\Delta(\tau) = -2$ for $\delta \in D_{p,0}$, or 2 otherwise.

With the preparation above, from (10) and combining with the case $r = 0$, we get

$$C_s(\tau) = \begin{cases} pq, & r = 0 \text{ and } \delta = 0, \\ p - q + 1, & r = 0 \text{ and } \delta \neq 0, \\ q - p - 3, & r \neq 0 \text{ and } \delta = 0, \\ 1, & r \in D_{q,0} \text{ and } \delta \in D_{p,1}, \text{ or } r \in D_{q,1} \text{ and } \delta \in D_{p,0}, \\ -3, & r \in D_{q,0} \text{ and } \delta \in D_{p,0}, \text{ or } r \in D_{q,1} \text{ and } \delta \in D_{p,1}. \end{cases} \quad (14)$$

Note that $\tau = vq + r$, $0 \leq v < p$, $0 \leq r < q$. By simple computation, we have (6) from (14). $\square$

5. Discussion and Conclusion

From the computation in the last section, it is the relation between two base sequences of $\mathbf{s}$ to ensure good autocorrelation. Therefore, other modified Jacobi sequences can be obtained by changing the companion pair. In addition, if we only change a few columns of $\mathbf{s}$, the autocorrelation of the corresponding sequence can also be obtained by making a few changes to the above equations. For example, we change the first column of $\mathbf{s}$ to $\mathbf{1}$ and the others do not change. The autocorrelation is not changed for $r = 0$. For $r \neq 0$, the term -2 in (10) should be changed to $+2$, and so the value of the autocorrelation should be added by 4. Thus, by (6) and (7), the autocorrelation of the resulting sequence is given as follows

1) If p is congruent to q modulo 4,

$$C_s(\tau) = \begin{cases} pq, & 1 \text{ time,} \\ p - q + 1, & q - 1 \text{ times,} \\ q - p + 1, & p - 1 \text{ times,} \\ 5, & (p - 1)(q - 1)/2 \text{ times,} \\ 1, & (p - 1)(q - 1)/2 \text{ times.} \end{cases}$$

2) If p is not congruent to q modulo 4,

$$C_s(\tau) = \begin{cases} pq, & 1 \text{ time,} \\ p - q + 1, & q - 1 \text{ times,} \\ q - p + 1, & p - 1 \text{ times,} \\ 3, & (p - 1)(q - 1) \text{ times.} \end{cases}$$

The autocorrelation values are also quite flat when $|p - q|$ is very small.

In this paper, we have studied the array structure of modified Jacobi sequences, which is called interleaved-like structure. Based on the structure, the autocorrelation of modified Jacobi sequences has been computed, and the essence has been revealed to get modifications of modified Jacobi sequences.

Acknowledgements

The authors would like to thank the anonymous reviewers for their helpful comments. The research is partially supported by Project of Hubei Provincial Department of Education (No. Q20101004).

References

- Brandstätter, N., Pirsic, G., & Winterhof, A. (2011). Correlation of the two-prime Sidel'nikov sequence. *Des. Codes Cryptogr*, 59, 59-68. <http://dx.doi.org/10.1007/s10623-010-9467-8>
- Calabro, D. (1968). On the synthesis of two-dimensional arrays with desirable correlation properties. *Information and Control*, 11(5-6), 537-560. [http://dx.doi.org/10.1016/s0019-9958\(67\)90755-3](http://dx.doi.org/10.1016/s0019-9958(67)90755-3)
- Cusick, T., Ding, C., & Renvall, A. (1998). *Stream Ciphers and Number Theory*. Amsterdam, the Netherlands: Elsevier/North-Holland.
- Ding, C. (1998). Autocorrelation values of generalized cyclotomic sequences of order two. *IEEE Transactions on Information Theory*, 44(4), 1699-1702. <http://dx.doi.org/10.1109/18.681354>
- Golomb, S. W., & Gong, G. (2005). *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*. New York: Cambridge Univ. Press.
- Gong, G. (1995). Theory and applications of q -ary interleaved sequences. *IEEE Transactions on Information Theory*, 41(2), 400-411. <http://dx.doi.org/10.1109/18.370141>
- Gong, G. (2002). New design for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ case. *IEEE Transactions on Information Theory*, 48(11), 2847-2867. <http://dx.doi.org/10.1109/TIT.2002.804044>
- Green, D. H., & Green, P. R. (2000). Modified Jacobi sequences. *IEE Proceeding Comput. Digit. Tech.*, 147(4), 241-251. <http://dx.doi.org/10.1049/ip-cdt:20000538>
- Li, S., Chen, Z., Fu, X., & Xiao, G. (2007). Autocorrelation values of new generalized cyclotomic sequences of order two and length pq . *Journal of Computer Science and Technology*, 22(6), 830-834. <http://dx.doi.org/10.1007/s11390-007-9099-2>
- Su, M., & Winterhof, A. (2010). Autocorrelation of Legendre-Sidelnikov sequences. *IEEE Transactions on Information Theory*, 56(4), 1714-1718. <http://dx.doi.org/10.1109/TIT.2010.2040893>
- Xiong, T., & Hall, J. I. (2011). Modifications of modified Jacobi sequences. *IEEE Transactions on Information Theory*, 57(1), 493-504. <http://dx.doi.org/10.1109/TIT.2010.2090271>

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>).