SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2018, Vol. 61 022308:1–022308:13
doi: 10.1007/s11432-016-9087-2

New quaternary sequences of even length with optimal auto-correlation

Wei SU[1,4], Yang YANG[2,4*], Zhengchun ZHOU[2] & Xiaohu TANG[3]

[1]*School of Economics and Information Engineering, Southwestern University of Finance and Economics, Chengdu* 610074*, China;*
[2]*School of Mathematics, Southwest Jiaotong University, Chengdu* 611756*, China;*
[3]*Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu* 611756*, China;*
[4]*Science and Technology on Communication Security Laboratory, Chengdu* 610041*, China*

Received 16 October 2016/Accepted 21 March 2017/Published online 11 October 2017

Abstract Sequences with low auto-correlation property have been applied in code-division multiple access communication systems, radar and cryptography. Using the inverse Gray mapping, a quaternary sequence of even length N can be obtained from two binary sequences of the same length, which are called component sequences. In this paper, using interleaving method, we present several classes of component sequences from twin-prime sequences pairs or GMW sequences pairs given by Tang and Ding in 2010; or two, three or four binary sequences defined by cyclotomic classes of order 4. Hence we can obtain new classes of quaternary sequences, which are different from known ones, since known component sequences are constructed from a pair of binary sequences with optimal auto-correlation or Sidel'nikov sequences.

Keywords binary sequences, quaternary sequences, Gray mapping, interleaving, cyclotomy

Citation Su W, Yang Y, Zhou Z C, et al. New quaternary sequences of even length with optimal auto-correlation. Sci China Inf Sci, 2018, 61(2): 022308, doi: 10.1007/s11432-016-9087-2

1 Introduction

Binary and quaternary sequences have received a lot of attention since they are easy to be implemented as multiple-access sequences in practical communication systems, radar, and cryptography [1, 2]. For example in some communication systems, in order to acquire the desired information from the received signals, the employed sequences are required to have auto-correlation values as low as possible so as to reduce the interference and noise. See [3] for a good survey paper on known constructions of binary and quaternary sequences with optimal auto-correlation.

Let $s = (s(0), s(1), \ldots, s(N-1))$ and $t = (t(0), t(1), \ldots, t(N-1))$ be two sequences of length N defined over the integer residue ring $\mathbb{Z}_H = \{0, 1, \ldots, H-1\}$. Then s is called a binary sequence if $H = 2$ or a quaternary sequence if $H = 4$. The support set of a binary sequence s is defined by the set $\{0 \leqslant i < N : s(i) = 1\}$.

The cross-correlation function $R_{s,t}(\tau)$ between s and t is defined by

$$R_{s,t}(\tau) = \sum_{i=0}^{N-1} \xi^{s(i)-t(i+\tau)}, \quad 0 \leqslant \tau < N,$$

* Corresponding author (email: yang_data@qq.com)

where $\xi = \exp(2\pi\sqrt{-1}/H)$ and the subscript $i + \tau$ is performed modulo N. If $s = t$, $R_{s,t}(\tau)$ is called the auto-correlation function of s, and denoted by $R_s(\tau)$ for short. The maximum out-of-phase auto-correlation magnitude of s is defined as

$$R_{\max}(s) = \max\{|R_s(\tau)| : 1 \leqslant \tau < N\}.$$

For a quaternary sequence s of odd length N, its maximum out-of-phase auto-correlation magnitude $R_{\max}(s)$ introduced above, is greater than or equal to 1, i.e., $R_{\max}(s) \geqslant 1$. Up to now, the only known class with $R_{\max}(s) = 1$ was proposed in [4]. This class of sequences has odd length $N = \frac{q+1}{2}$ and is constructed from odd perfect sequences [5] of length $q + 1$, where $q \equiv 1 (\mathrm{mod}\ 4)$ is an odd prime power. The next smallest values for the maximum out-of-phase auto-correlation magnitude of a quaternary sequence of odd length are as follows:

- $R_{\max}(s) = \sqrt{5}$ for $N \equiv 1 (\mathrm{mod}\ 4)$ [6–10];
- $R_{\max}(s) = 3$ for $N \equiv 3 (\mathrm{mod}\ 4)$ [7, 11].

Those constructions are mainly based on cyclotomy or interleaving technique [2].

For the case of even length N, a sequence s is called optimal if $R_{\max}(s) = 2$ [12]. In [13, 14], optimal quaternary sequences of length $q - 1$ were obtained from Sidel'nikov sequences, q being an odd prime power. Using the inverse Gray mapping, a quaternary sequence of even length can be obtained from two binary sequences of the same length, which are called component sequences in this paper. Several constructions of component sequences via interleaving Legendre sequences [15], or binary sequences with ideal auto-correlation [16], were presented to design optimal quaternary sequences. By extending the constructions in [15, 16], Tang and Ding [12] developed a generic construction of component sequences which works for any pair of ideal sequences of the same length.

The objective of this paper is to obtain new more component sequences via interleaving technique. It will be seen later that the resultant component sequences include a pair of non-ideal sequences, and lead to new optimal quaternary sequences under the inverse Gray mapping. More precisely, our two binary component sequences can be defined by the following sequences:

- Twin-prime sequences pairs and GMW sequences pairs given by Tang and Gong in 2010 [17].
- Two, three or four binary sequences defined by cyclotomic classes of order 4 with respect to the integer residue ring $\mathbb{Z}_n$, n begin an odd prime.

Compared with optimal quaternary sequences given by [12,13,15,16], ours have different auto-correlation functions. Examples applying non-ideal sequences to design optimal quaternary sequences are also given.

This paper is organized as follows. In Section 2, interleaving method and Gray mapping will be briefly introduced. In Section 3, using the inverse Gray mapping to two binary sequences, a generic construction of quaternary sequences of even length will be proposed. In Section 4, as an application of the generic construction, we first recall known constructions of component sequences, and then present some new component sequences derived from GMW sequences pairs and twin-prime sequences pairs given in [17] and by using two, three and four different sequences defined by cyclotomic classes of order 4 with respect to the integer residue ring $\mathbb{Z}_n$, n being an odd prime, respectively. In Section 5, we will give three examples to illustrate our results. Finally, some concluding remarks will be given in Section 6.

2 Preliminaries

2.1 Interleaved sequences of length $2n$

In this subsection, we briefly introduce to the representation of an interleaved sequence of length $2n$. Please refer to [2] for more details for the interleaving method.

Let n be a positive integer. Assume that $a_i = (a_i(0), a_i(1), \ldots, a_i(n-1))$ is a sequence of length n,

$i = 0, 1$, and $g = (g_0, g_1)$ is a sequence defined over $\mathbb{Z}_n$. Define a matrix $(u_{i,j})_{n\times 2}$:

$$(u_{i,j})_{n\times 2} = \begin{pmatrix} a_0(g_0) & a_1(g_1) \\ a_0(g_0+1) & a_1(g_1+1) \\ \vdots & \vdots \\ a_0(g_0+n-1) & a_1(g_1+n-1) \end{pmatrix}.$$

Concatenating the successive rows of the matrix above, an interleaved sequence u of length $2n$ is obtained as follows:

$$u(2i+j) = u_{i,j}, \quad 0 \leqslant i < N, \quad 0 \leqslant j < 2.$$

For convenience, denote u as

$$u = I(L^{g_0}(a_0), L^{g_1}(a_1)),$$

where I is the interleaving operator, and $L^{g_i}(a_i) = (a_i(g_i), a_i(g_i+1), \ldots, a_i(g_i+n-1))$. The sequences a_0 and a_1 are called the column sequences of u. Let

$$v = (L^{f_0}(b_0), L^{f_1}(b_1)).$$

Consider the τ shifted version $L^\tau(v)$ of v, where $\tau = 2\tau_1 + \tau_2$ $(0 \leqslant \tau_1 < n, 0 \leqslant \tau_2 < 2)$, we have

$$L^\tau(v) = \begin{cases} I(L^{f_0+\tau_1}(b_0), L^{f_1+\tau_1}(b_1)), & \tau = 2\tau_1, \\ I(L^{f_1+\tau_1}(b_1), L^{f_0+\tau_1+1}(b_0)), & \tau = 2\tau_1+1. \end{cases}$$

It then follows that the cross-correlation function between u and v at the shift τ is given by

$$R_{u,v}(\tau) = \begin{cases} R_{a_0,b_0}(\tau_1 + f_0 - g_0) + R_{a_1,b_1}(\tau_1 + f_1 - g_1), & \tau = 2\tau_1, \\ R_{a_0,b_1}(\tau_1 + f_1 - g_0) + R_{a_1,b_0}(\tau_1 + 1 + f_0 - g_1), & \tau = 2\tau_1 + 1. \end{cases} \tag{1}$$

2.2 Gray mapping

The well-known Gray mapping $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ is defined as

$$\phi(0) = (0,0), \quad \phi(1) = (0,1), \quad \phi(2) = (1,1), \quad \phi(3) = (1,0).$$

Using the inverse Gray mapping $\phi^{-1} : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$, i.e.,

$$\phi^{-1}(0,0) = 0, \quad \phi^{-1}(0,1) = 1, \quad \phi^{-1}(1,1) = 2, \quad \phi^{-1}(1,0) = 3,$$

any quaternary sequence $u = (u(0), u(1), \ldots, u(N-1))$ can be obtained from two binary sequences $c = (c(0), c(1), \ldots, c(N-1))$ and $d = (d(0), d(1), \ldots, d(N-1))$ as follows:

$$u(i) = \phi^{-1}(c(i), d(i)), \quad 0 \leqslant i < N. \tag{2}$$

Here the binary sequences c and d are called component sequences of u.

Transforming the sequence u into its complex valued version,

$$\xi^{u(i)} = \frac{1}{2}(1+\xi)(-1)^{c(i)} + \frac{1}{2}(1-\xi)(-1)^{d(i)}, \quad 0 \leqslant i < N,$$

where $\xi = \sqrt{-1}$, Krone and Sarwate [18] observed the following result.

Lemma 1 ([18]). The auto-correlation function of u is given by

$$R_u(\tau) = \frac{1}{2}(R_c(\tau) + R_d(\tau)) + \frac{\xi}{2}(R_{c,d}(\tau) - R_{d,c}(\tau)), \quad 0 \leqslant \tau < N. \tag{3}$$

3 Generic construction of quaternary sequences

In this section, we present a procedure for the construction of quaternary sequences with optimal auto-correlation.

Construction I: Construction of quaternary sequence via Gray mapping.

(1) Let n be an odd integer, $N = 2n$, and $\lambda = \frac{n+1}{2}$. Generate four binary sequences a_i of length n, $0 \leqslant i \leqslant 3$, and a binary sequence $e = (e(0), e(1), e(2))$, $e(j) = 0, 1$.

(2) Define two binary sequences of length N:

$$c = I(a_0, e(0) + L^\lambda(a_1)), \quad d = I(e(1) + a_2, e(2) + L^\lambda(a_3)), \tag{4}$$

where $L^\lambda(b) + 1$ denotes the complement of the sequence $L^\lambda(b) = (b(\lambda), b(\lambda+1), \ldots, b(\lambda+n-1))$, i.e., $L^\lambda(b) + 1 = (b(\lambda)+1, b(\lambda+1)+1, \ldots, b(\lambda+n-1)+1)$.

(3) Applying the inverse Gray mapping ϕ^{-1} to c and d, obtain a quaternary sequence u of length N, where $u(i) = \phi^{-1}(c(i), d(i))$.

We have the following result.

Theorem 1. The auto-correlation of u generated by Construction I is given by

$$\begin{aligned} R_u(\tau) \,=\, & [R_{a_0}(\tau_0) + R_{a_1}(\tau_0) + R_{a_2}(\tau_0) + R_{a_3}(\tau_0)]/2 \\ & +(-1)^{e(1)}[R_{a_0,a_2}(\tau_0) - R_{a_2,a_0}(\tau_0) + (-1)^{e(0)+e(1)+e(2)}(R_{a_1,a_3}(\tau_0) - R_{a_3,a_1}(\tau_0))]\xi/2, \end{aligned}$$

if $\tau = 2\tau_0$, and

$$\begin{aligned} R_u(\tau) \,=\, & (-1)^{e(0)}[R_{a_0,a_1}(\tau_2) + R_{a_1,a_0}(\tau_2) + (-1)^{e(0)+e(1)+e(2)}(R_{a_2,a_3}(\tau_2) + R_{a_3,a_2}(\tau_2))]/2 \\ & +(-1)^{e(2)}[R_{a_0,a_3}(\tau_2) - R_{a_3,a_0}(\tau_2) + (-1)^{e(0)+e(1)+e(2)}(R_{a_1,a_2}(\tau_2) - R_{a_2,a_1}(\tau_2))]\xi/2, \end{aligned}$$

if $\tau = 2\tau_0 + 1$, where $\tau_2 = \tau_0 + \lambda$.

Proof. Calculate the auto-correlation and cross-correlation functions of c and d. Writing $\tau = 2\tau_0 + \tau_1$, where $0 \leqslant \tau_0 < n$ and $\tau_1 = 0, 1$, we consider the auto-correlation of c in two cases according to $\tau_1 = 0$ and $\tau_1 = 1$.

Case 1: $\tau_1 = 0$, by (1), in this case we have

$$R_c(\tau) \,=\, R_{a_0}(\tau_0) + R_{a_1}(\tau_0).$$

Case 2: $\tau_1 = 1$, by (1) again, we have

$$\begin{aligned} R_c(\tau) \,&=\, (-1)^{e(0)} R_{a_0,a_1}(\tau_0 + \lambda) + (-1)^{e(0)} R_{a_1,a_0}(\tau_0 + 1 - \lambda), \\ &=\, (-1)^{e(0)}(R_{a_0,a_1}(\tau_0 + \lambda) + R_{a_1,a_0}(\tau_0 + \lambda)), \end{aligned}$$

where the second identity was due to $(\tau_0 + 1 - \lambda) \equiv (\tau_0 + \lambda) (\mathrm{mod}\ n)$. The following correlation functions can be similarly proved:

$$R_d(\tau) = \begin{cases} R_{a_2}(\tau_0) + R_{a_3}(\tau_0), & \tau = 2\tau_0, \\ (-1)^{e(1)+e(2)}(R_{a_2,a_3}(\tau_0 + \lambda) + R_{a_3,a_2}(\tau_0 + \lambda)), & \tau = 2\tau_0 + 1, \end{cases}$$

$$R_{c,d}(\tau) = \begin{cases} (-1)^{e(1)} R_{a_0,a_2}(\tau_0) + (-1)^{e(0)+e(2)} R_{a_1,a_3}(\tau_0), & \tau = 2\tau_0, \\ (-1)^{e(2)} R_{a_0,a_3}(\tau_0 + \lambda) + (-1)^{e(0)+e(1)} R_{a_1,a_2}(\tau_0 + \lambda), & \tau = 2\tau_0 + 1, \end{cases}$$

$$R_{d,c}(\tau) = \begin{cases} (-1)^{e(1)} R_{a_2,a_0}(\tau_0) + (-1)^{e(0)+e(2)} R_{a_3,a_1}(\tau_0), & \tau = 2\tau_0, \\ (-1)^{e(2)} R_{a_3,a_0}(\tau_0 + \lambda) + (-1)^{e(0)+e(1)} R_{a_2,a_1}(\tau_0 + \lambda), & \tau = 2\tau_0 + 1. \end{cases}$$

The conclusion then follows from (3) and the discussion above.

Corollary 1. Let a_0, a_1, a_2, a_3 be four binary sequences of odd length n and $e = (e(0), e(1), e(2))$ be a binary sequence. Then $R_{\max}(u) = 2$, if

$$\begin{cases} R_{a_0}(\tau_0) + R_{a_1}(\tau_0) + R_{a_2}(\tau_0) + R_{a_3}(\tau_0) \in \{0, \pm 4\}, & 1 \leqslant \tau_0 < n, \\ R_{a_0,a_2}(\tau_0) - R_{a_2,a_0}(\tau_0) + (-1)^{e(0)+e(1)+e(2)}(R_{a_1,a_3}(\tau_0) - R_{a_3,a_1}(\tau_0)) = 0, & 1 \leqslant \tau_0 < n, \\ R_{a_0,a_1}(\tau_0) + R_{a_1,a_0}(\tau_0) + (-1)^{e(0)+e(1)+e(2)}(R_{a_2,a_3}(\tau_0) + R_{a_3,a_2}(\tau_0)) \in \{0, \pm 4\}, & 0 \leqslant \tau_0 < n, \\ R_{a_0,a_3}(\tau_0) + R_{a_3,a_0}(\tau_0) + (-1)^{e(0)+e(1)+e(2)}(R_{a_1,a_2}(\tau_0) - R_{a_2,a_1}(\tau_0)) = 0, & 0 \leqslant \tau_0 < n. \end{cases} \tag{5}$$

Proof. If Eq. (5) holds, then by Theorem 1,

$$R_u(\tau) = [R_{a_0}(\tau_0) + R_{a_1}(\tau_0) + R_{a_2}(\tau_0) + R_{a_3}(\tau_0)]/2 \in \{0, \pm 2\},$$

if $\tau = 2\tau_0$, and

$$R_u(\tau) = (-1)^{e(0)}[R_{a_0,a_1}(\tau') + R_{a_1,a_0}(\tau') + (-1)^{e(0)+e(1)+e(2)}(R_{a_2,a_3}(\tau') + R_{a_3,a_2}(\tau'))]/2 \in \{0, \pm 2\},$$

if $\tau = 2\tau_0 + 1$, where $\tau' = \tau_0 + \lambda$. Hence $R_u(\tau) \in \{0, \pm 2\}$ for all $1 \leqslant \tau < N$, i.e., u is optimal.

4 Quaternary sequences from the generic construction

In this section, we will show that our generic construction includes some known constructions of optimal quaternary sequences as special cases, and can produce new quaternary sequences with optimal auto-correlation. Throughout this section, suppose that u is the quaternary sequence generated by Construction L.

4.1 Known constructions of a_0, a_1, a_2, a_3

Theorem 2 ([16]). Let $a_0 = a_1 = a_2 = a_3$, which are the same ideal sequences of length $n = 2^m - 1$, and $e = (0, 0, 1)$. Then u is an optimal quaternary sequence, and for $1 \leqslant \tau < 2n$,

$$R_u(\tau) = \begin{cases} -2, & \tau = 2\tau_0, \\ 0, & \tau = 2\tau_0 + 1. \end{cases}$$

Theorem 2 was generalized by Tang and Ding as follows.

Theorem 3 ([12]). Let $a_0 = a_1$ and $a_2 = a_3$ be ideal sequences of the same length n, i.e., $R_{a_0}(\tau_0) = R_{a_2}(\tau_0) = -1$, $1 \leqslant \tau_0 < n$. Let $e = (0, 0, 1)$. Then u is an optimal quaternary sequence with auto-correlation function

$$R_u(\tau) = \begin{cases} -2, & \tau = 2\tau_0, \\ 0, & \tau = 2\tau_0 + 1. \end{cases}$$

In [12,15], the following result has been obtained by choosing the Legendre sequences pair (please refer to [17] for more details).

Theorem 4 ([12,15]). Let s and t be the Legendre sequences pair of odd prime length n. Let $e = (0, 0, 1)$ and

$$(a_0, a_1, a_2, a_3) \in \{(s, t, s, t), (s, t, t, s), (t, s, t, s), (t, s, s, t)\}.$$

Then u is an optimal quaternary sequence with auto-correlation function

$$R_u(\tau) = \begin{cases} -2, & \tau = 2\tau_0, \\ 0, & \tau = 2\tau_0 + 1. \end{cases}$$

Remark 1. From known constructions above, a_0, a_1, a_2, a_3 were defined by one or two binary sequences with optimal auto-correlation. In the next subsections, we will present new constructions of a_0, a_1, a_2, a_3, some of which have non-optimal auto-correlation functions. Those new a_0, a_1, a_2, a_3 satisfy (5), and can be used to obtain optimal quaternary sequences u.

4.2 New constructions of a_0, a_1, a_2, a_3 using a sequence pair

Using the twin-prime sequences pairs and the GMW-sequences pairs given in [17], the following results can be obtained from Corollary 1.

Theorem 5. Let s and t be the twin-prime sequences pair of length $p(p+2)$. Let $e = (e(0), e(1), e(2))$ satisfy $e(0) + e(1) + e(2) \equiv 1 (\mathrm{mod}\ 2)$ and

$$(a_0, a_1, a_2, a_3) \in \{(s,t,s,t), (s,t,t,s), (t,s,t,s), (t,s,s,t)\}.$$

Then u given by Construction I is an optimal quaternary sequence with auto-correlation function

$$R_u(\tau) = \begin{cases} -2, & \tau = 2\tau_0, \quad \tau_0 \equiv 0 (\mathrm{mod}\ p+2), \\ 2, & \tau = 2\tau_0, \quad \tau_0 \not\equiv 0 (\mathrm{mod}\ p+2), \\ 0, & \tau = 2\tau_0 + 1. \end{cases}$$

Theorem 6. Let s and t be the GMW sequences pair of length $2^{2k} - 1$. Let $e = (e(0), e(1), e(2))$ satisfy $e(0) + e(1) + e(2) \equiv 1 (\mathrm{mod}\ 2)$ and

$$(a_0, a_1, a_2, a_3) \in \{(s,t,s,t), (s,t,t,s), (t,s,t,s), (t,s,s,t)\}.$$

Then u given by Construction I is an optimal quaternary sequence with auto-correlation function

$$R_u(\tau) = \begin{cases} -2, & \tau = 2\tau_0, \quad \tau_0 \equiv 0 (\mathrm{mod}\ 2^k+1), \\ 2, & \tau = 2\tau_0, \quad \tau_0 \not\equiv 0 (\mathrm{mod}\ 2^k+1), \\ 0, & \tau = 2\tau_0 + 1. \end{cases}$$

Remark 2. By choosing the twin-prime sequences pairs and GMW sequences pairs, the quaternary sequence u given by Construction I is different from the quaternary sequence given by Theorem 6 of [12], since the auto-correlation function of our sequence take values $0, \pm 2$, and that of the sequence in [12] takes values $0, -2$.

4.3 Constructions of a_0, a_1, a_2, a_3 using cyclotomic classes of order 4

Assume that $n = 4f + 1 = x^2 + 4y^2$ is an odd prime, where f, x and y are integers. Let D_0, D_1, D_2, D_3 be the cyclotomic classes of order 4 with respect to $\mathbb{Z}_n$ (See Appendix A). Let $s_1, s_2, s_3, s_4, s_5, s_6$ be six binary sequences of length n with support sets $D_0 \cup D_1$, $D_0 \cup D_2$, $D_0 \cup D_3$, $D_1 \cup D_2$, $D_1 \cup D_3$, $D_2 \cup D_3$, respectively.

In this subsection, we will present new constructions of a_0, a_1, a_2, a_3 choosing from $s_1, s_2, s_3, s_4, s_5, s_6$, whose auto-correlation and cross-correlation functions are given in Appendix A. The following discussion are divided into two cases: f odd and f even.

Theorem 7. Let f be odd, and $y = -1$. Let $e = (e(0), e(1), e(2))$ satisfy $e(0) + e(1) + e(2) \equiv 0 (\mathrm{mod}\ 2)$ and

$$(a_0, a_1, a_2, a_3) \in \left\{ \begin{array}{l} (s_2, s_1, s_2, s_1), (s_1, s_2, s_1, s_2), (s_6, s_2, s_6, s_2), (s_2, s_6, s_2, s_6), \\ (s_5, s_4, s_5, s_4), (s_4, s_5, s_4, s_5), (s_3, s_5, s_3, s_5), (s_5, s_3, s_5, s_3) \end{array} \right\}.$$

Then u given by Construction I is an optimal quaternary sequence, i.e., for $1 \leqslant \tau < 2n$, $R_u(\tau) = \pm 2$.

Proof. Note that $a_0 = a_2$ and $a_1 = a_3$, where $(a_0, a_1) \in \{(s_2, s_1), (s_1, s_2), (s_6, s_2), (s_2, s_6), (s_5, s_4), (s_4, s_5), (s_3, s_5), (s_5, s_3)\}$. By Theorem 1, the auto-correlation function of u is reduced as

$$R_u(\tau) = \begin{cases} R_{a_0}(\tau_0) + R_{a_1}(\tau_0), & \tau = 2\tau_0, \\ (-1)^{e(0)}[R_{a_0,a_1}(\tau_0 + \lambda) + R_{a_1,a_0}(\tau_0 + \lambda)], & \tau = 2\tau_0 + 1. \end{cases}$$

Using the values of auto-correlation and cross-correlation functions of a_0 and a_1 obtained in Lemma 3 and Theorem 11 in Appendix A, the result follows immediately.

Theorem 8. Let f be odd, and $y=-1$. Let $e=(e(0),e(1),e(2))$ with $e(0)+e(1)+e(2)\equiv 0(\mathrm{mod}\ 2)$ and

$$(a_0,a_1,a_2,a_3)\in\left\{\begin{array}{l}(s_1,s_2,s_2,s_1),(s_2,s_1,s_1,s_2),(s_2,s_6,s_6,s_2),(s_6,s_2,s_2,s_6),\\(s_4,s_5,s_5,s_4),(s_5,s_4,s_4,s_5),(s_5,s_3,s_3,s_5),(s_3,s_5,s_5,s_3)\end{array}\right\}.$$

Then u given by Construction I is an optimal quaternary sequence, i.e., for $1\leqslant\tau<2n$, $R_u(\tau)=\pm 2$.

Proof. Note that $a_0=a_3$ and $a_1=a_2$, where $(a_0,a_1)\in\{(s_2,s_1),(s_1,s_2),(s_6,s_2),(s_2,s_6),(s_5,s_4),(s_4,s_5),(s_3,s_5),(s_5,s_3)\}$. By Theorem 1, the auto-correlation function of u is reduced as

$$R_u(\tau)=\left\{\begin{array}{ll}R_{a_0}(\tau_0)+R_{a_1}(\tau_0), & \tau=2\tau_0,\\(-1)^{e(0)}[R_{a_0,a_1}(\tau_0+\lambda)+R_{a_1,a_0}(\tau_0+\lambda)], & \tau=2\tau_0+1.\end{array}\right.$$

Based on the auto-correlation and cross-correlation functions of a_0 and a_1 obtained in Lemma 3 and Theorem 11 in Appendix A, the result follows immediately.

Theorem 9. Let f be odd and $y=-1$. Let $e=(e(0),e(1),e(2))$ with $e(0)+e(1)+e(2)\equiv 1(\mathrm{mod}\ 2)$ and

$$(a_0,a_1,a_2,a_3)\in\left\{\begin{array}{l}(s_2,s_1,s_6,s_2),(s_2,s_6,s_1,s_2),(s_5,s_3,s_4,s_5),(s_5,s_4,s_3,s_5),\\(s_6,s_2,s_2,s_1),(s_1,s_2,s_2,s_6),(s_3,s_5,s_5,s_4),(s_4,s_5,s_5,s_3)\end{array}\right\}.$$

Then u given by Construction I is an optimal quaternary sequence, i.e., for $1\leqslant\tau<2n$, $R_u(\tau)=\pm 2$.

Proof. By Theorem 1, the result follows immediately by using the auto-correlation and cross-correlation functions of s_1,s_3,s_4 and s_6 given in Lemma 3 and Theorem 11 in Appendix A.

Theorem 10. Let f be even and $x=\pm 1$. Let $e=(e(0),e(1),e(2))$ with $e(0)+e(1)+e(2)\equiv 0(\mathrm{mod}\ 2)$ and

$$(a_0,a_1,a_2,a_3)\in\left\{\begin{array}{l}(s_6,s_3,s_4,s_1),(s_6,s_4,s_3,s_1),(s_4,s_6,s_3,s_1),(s_3,s_6,s_4,s_1),\\(s_4,s_1,s_6,s_3),(s_6,s_4,s_1,s_3),(s_1,s_4,s_6,s_3),(s_4,s_6,s_1,s_3),\\(s_3,s_1,s_6,s_4),(s_6,s_3,s_1,s_4),(s_1,s_3,s_6,s_4),(s_3,s_6,s_1,s_4),\\(s_4,s_1,s_3,s_6),(s_3,s_1,s_4,s_6),(s_1,s_3,s_4,s_6),(s_1,s_4,s_3,s_6)\end{array}\right\}.$$

Then u given by Construction I is an optimal quaternary sequence, i.e., for $1\leqslant\tau<2n$, $R_u(\tau)=\pm 2$.

Proof. Note that for any $i\neq j$, $R_{s_i,s_j}(\tau)=R_{s_j,s_i}(\tau)$ holds for all $0\leqslant\tau<n$ (see Lemma 3 in Appendix A). That is to say, $0\leqslant i\neq j\leqslant 3$, $R_{a_i,a_j}(\tau)=R_{a_j,a_i}(\tau)$ holds for all $0\leqslant\tau<n$. Hence by Theorem 1, the auto-correlation function of u is given by

$$R_u(\tau)=\left\{\begin{array}{ll}[R_{a_0}(\tau_0)+R_{a_1}(\tau_0)+R_{a_2}(\tau_0)+R_{a_3}(\tau_0)]/2, & \tau=2\tau_0,\\(-1)^{e(0)}[R_{a_0,a_1}(\tau_0+\lambda)+R_{a_2,a_3}(\tau_0+\lambda)], & \tau=2\tau_0+1.\end{array}\right.$$

The result follows immediately from the auto-correlation and cross-correlation functions of s_1,s_3,s_4 and s_6 given by Lemma 3 and Theorem 12 in Appendix A.

5 Examples

In this section, we will give three examples of our new constructions of quaternary sequences with optimal auto-correlation.

Example 1. Define two binary sequences of length 25 as follows:

$$a_0=a_2=(0,0,0,1,1,1,0,1,0,1,1,0,1,0,1,1,0,1,0,1,1,1,0,0,0),$$
$$a_1=a_3=(1,0,0,1,1,0,1,0,0,0,0,0,1,0,0,0,0,0,1,0,1,1,0,0,1).$$

With the help of Magma Program, the auto-correlation and cross-correlation functions of a_0 and a_1 are given by

$$\begin{aligned}
&(R_{a_0}(\tau))_{\tau=0}^{24} = (25,-3,5,-3,-7,5,-7,1,-3,1,1,1,-3,-3,1,1,1,-3,1,-7,5,-7,-3,5,-3),\\
&(R_{a_1}(\tau))_{\tau=0}^{24} = (25,1,-3,5,5,-3,5,1,5,1,-3,-3,1,1,-3,-3,1,5,1,5,-3,5,5,-3,1),\\
&(R_{a_0,a_1}(\tau))_{\tau=0}^{24} = (1,1,-7,1,-3,-3,-3,-3,5,5,1,5,-3,-3,5,1,5,5,-3,-3,-3,-3,1,-7,1),\\
&(R_{a_1,a_0}(\tau))_{\tau=0}^{24} = (1,1,-7,1,-3,-3,-3,-3,5,5,1,5,-3,-3,5,1,5,5,-3,-3,-3,-3,1,-7,1).
\end{aligned}$$

It can be seen that both a_0 and a_1 are non-ideal sequences. By Theorem 1, we can obtain a quaternary sequence

$$\begin{aligned}
u = {} & (0,1,0,1,0,1,2,1,2,1,2,3,0,1,2,3,0,3,2,1,2,1,0,3,2,3,0,1,2,\\
& 1,2,3,0,3,2,1,0,3,2,1,2,1,2,1,0,1,0,1,0,3)
\end{aligned}$$

with auto-correlation

$$\begin{aligned}
(R_u(\tau))_{\tau=1}^{49} = {} & (0,-2,0,2,0,2,0,-2,0,2,0,-2,0,2,0,2,0,2,0,-2,0,\\
& -2,0,-2,0,-2,0,-2,0,-2,0,2,0,2,0,2,0,-2,0,2,0,-2,0,2,0,2,0,-2,0).
\end{aligned}$$

Example 2. Let α be a primitive element of the finite field F_{2^6} generated by the primitive polynomial $f(x) = x^6 + x + 1$ and $f(\alpha) = 0$. Let $a_0 = (a_0(0), a_0(1), \ldots, a_0(62))$ be the m-sequence of length 63, where $a_0(i) = Tr_1^6(\alpha^i) = \alpha^i + \alpha^{2i} + \alpha^{4i} + \alpha^{8i} + \alpha^{16i} + \alpha^{32i}$, i.e.,

$$\begin{aligned}
a_0 = a_2 = {} & (0,0,0,0,0,1,0,0,0,0,1,1,0,0,0,1,0,1,0,0,1,1,1,1,0,1,0,0,0,1,1,1,0,0,1,\\
& 0,0,1,0,1,1,0,1,1,1,0,1,1,0,0,1,1,0,1,0,1,0,1,1,1,1,1,1).
\end{aligned}$$

and its modification a_1 given in [17] equal to

$$\begin{aligned}
a_1 = a_3 = {} & (1,0,0,0,0,1,0,0,0,1,1,1,0,0,0,1,0,1,1,0,1,1,1,1,0,1,0,1,0,1,1,1,0,0,1,\\
& 0,1,1,0,1,1,0,1,1,1,1,1,1,0,0,1,1,0,1,1,1,0,1,1,1,1,1,1).
\end{aligned}$$

Then by Theorem 6, we have

$$\begin{aligned}
u = {} & (0,1,0,1,0,3,0,1,0,3,2,3,0,1,0,3,0,3,0,1,2,3,2,3,0,3,0,3,0,3,2,3,0,1,2,\\
& 1,0,3,0,3,2,1,2,3,2,3,2,3,0,1,2,3,0,3,0,3,0,3,2,3,2,3,2,3,0,1,0,1,2,1,\\
& 0,1,0,3,2,1,0,1,2,1,2,3,0,3,2,3,2,1,2,1,0,1,2,3,2,1,0,3,0,3,2,1,2,3,0,\\
& 3,2,3,0,3,2,1,0,3,2,1,2,3,2,1,2,3,2,3,2,3).
\end{aligned}$$

Hence we have

$$\begin{aligned}
(R_u(\tau))_{\tau=1}^{125} = {} & (0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,-2,0,2,0,2,0,2,0,2,0,2,0,\\
& 2,0,2,0,2,0,-2,0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,-2,0,2,\\
& 0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,-2,0,2,0,2,0,2,0,2,0,2,0,2,2,0,\\
& 2,0,0,-2,0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,2,0,-2,0,2,0,2,0,2,0,2,\\
& 0,2,0,2,0,2,0,2,0).
\end{aligned}$$

i.e., the out-of-phase auto-correlation of u takes values $0, \pm 2$.

Example 3. Let $\alpha = 3$ be a generator of the multiplicative group of the integer residue ring $\mathbb{Z}_{17}$. Then the cyclotomic classes of order 4 with respect to $\mathbb{Z}_{17}$ are given as follows:

$$\begin{aligned}
C_0 = {} & \{1,4,13,16\}, \quad C_1 = \{3,5,12,14\},\\
C_2 = {} & \{2,8,9,15\}, \quad C_3 = \{6,7,10,11\}.
\end{aligned}$$

It is easy to check that the following sequences

$$\begin{aligned} s_1 &= (0,1,0,1,1,1,0,0,0,0,0,0,1,1,1,0,1),\\ s_3 &= (0,1,0,0,1,0,1,1,0,0,1,1,0,1,0,0,1),\\ s_4 &= (0,0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0),\\ s_6 &= (0,0,1,0,0,0,1,1,1,1,1,1,0,0,0,1,0) \end{aligned}$$

with support sets $C_0 \cup C_1$, $C_0 \cup C_3$, $C_1 \cup C_2$ and $C_2 \cup C_3$ respectively are non-optimal binary sequences of length 17. Take $a_0 = s_6$, $a_1 = s_3$, $a_2 = s_4$, $a_4 = s_1$, and $e = (0,0,0)$. By Theorem 10, the quaternary sequence u is equal to

$$u = (0,0,0,3,2,3,1,1,0,2,1,1,3,0,3,2,2,0,2,2,3,0,3,1,1,2,0,1,1,3,2,3,0,0),$$

which has the out-of-phase auto-correlation function:

$$\begin{aligned} (R_u(\tau))_{\tau=1}^{33} = (&2,-2,-2,-2,-2,-2,-2,-2,2,-2,-2,-2,2,-2,2,\\ &-2,2,-2,2,-2,2,-2,-2,-2,2,-2,-2,-2,-2,-2,-2,2). \end{aligned}$$

6 Conclusion

Using the inverse Gray mapping and interleaving method, the authors in [12] proposed a construction of multiple-access quaternary sequences of even length with optimal magnitude by choosing arbitrary two ideal sequences of the same length, which is a generalization of [15,16]. While in this paper, we construct component sequences via interleaving: twin-prime sequences pairs and GMW sequences pairs given by Tang and Gong in 2010; or two, three or four binary sequences defined by cyclotomic classes of order 4. Compared with those sequences given in [12], our proposed sequences can be defined by using non-ideal binary sequences and have different auto-correlation functions.

Acknowledgements The work of Wei SU was supported by National Science Foundation of China (Grant No. 61402377), and in part supported by Open Research Subject of Key Laboratory (Research Base) of Digital Space Security (Grant No. szjj2014-075), and Science and Technology on Communication Security Laboratory (Grant No. 9140C110302150C11004). The work of Yang YANG was supported by National Science Foundation of China (Grants Nos. 61401376, 11571285), and Application Fundamental Research Plan Project of Sichuan Province (Grant No. 2016JY0160). The work of Zhengchun ZHOU and Xiaohu TANG was supported by National Science Foundation of China (Grants Nos. 61672028, 61325005).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Fan P Z, Darnell M. Sequences Design for Communication Applications. Australia and New Zealand: Jacaranda Wiley Ltd., 1996. 5–15
2 Golomb S W, Gong G. Signal Design for Good Correlation: for Wireless Communication. Cambridge: Cryptography and Radar Cambridge University Press, 2005. 1–438
3 Lüke H D, Schotten H D, Hadinejad-Mahram H. Binary and quadriphase sequence with optimal autocorrelation: a survey. IEEE Trans Inf Theory, 2003, 49: 3271–3282
4 Schotten H D. Optimum complementary sets and quadriphase sequences derived form q-ary m-sequences. In: Proceedings of IEEE International Symposium on Information Theory, Ulm, 1997. 485
5 Lüke H D, Schotten H D. Odd-perfect almost binary correlation sequences. IEEE Trans Aerosp Electron Syst, 1995, 31: 495–498
6 Green D H, Green P R. Polyphase-related prime sequences. IEEE Proc Comput Digit Tech, 2001, 148: 53–62
7 Li N, Tang X H, Helleseth T. New M-ary sequences with low autocorrelation from interleaved technique. Des Codes Cryptogr, 2014, 73: 237–249
8 Sidelnikov V M. Some k-vauled pseudo-random sequences and nearly equidistant codes. Probl Inf Trans, 1969, 5: 12–16

9 Tang X H, Lindner J. Almost quadriphase sequence with ideal autocorrelation property. IEEE Signal Process Lett, 2009, 16: 38–40
10 Yang Z, Ke P H. Quaternary sequences with odd period and low autocorrelation. Electron Lett, 2010, 46: 1068–1069
11 Yang Z, Ke P H. Construction of quaternary sequences of length pq with low autocorrelation. Cryptogr Commun Discret Struct Boolean Funct Seq, 2011, 3: 55–64
12 Tang X H, Ding C. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value. IEEE Trans Inf Theory, 2010, 56: 6398–6405
13 Kim Y-S, Jang J-W, Kim S-H, et al. New quaternary sequences with optimal autocorrelation. In: Proceedings of the IEEE International Conference on Symposium on Information Theory, Seoul, 2009. 286–289
14 Lüke H D, Schotten H D, Hadinejad-Mahram H. Generalised Sidelnikov sequences with optimal autocorrelation properties. Electron Lett, 2000, 36: 525–527
15 Kim Y-S, Jang J-W, Kim S-H, et al. New construction of quaternary sequences with ideal autocorrelation from Legendre sequences. In: Proceedings of the IEEE international conference on Symposium on Information Theory, Seoul, 2009. 282–285
16 Jang J W, Kim Y S, Kim S H, et al. New quaternary sequences with ideal autocorrelation constructed from binary sequences with ideal autocorrelation. In: Proceedings of IEEE International Symposium on Information Theory, Seoul, 2009. 278–281
17 Tang X H, Gong G. New constructions of binary sequences with optimal autocorrelation value/magnitude. IEEE Trans Inf Theory, 2010, 56: 1278–1286
18 Krone S M, Sarwate D V. Quadriphase sequences for spread spectrum multiple access communication. IEEE Trans Inf Theory, 1984, IT-30: 520–529

Appendix A Auto-correlation and cross-correlation of $s_i, 1 \leqslant i \leqslant 6$

In this section, we will first review the cyclotomic classes of order 4 and then discuss the auto-correlation and cross-correlation of s_i defined by cyclotomic classes.

Assume that $n = 4f + 1 = x^2 + 4y^2$ is a prime, where f, x and y are integers. Let α be a generator of the multiplicative group of the integer residue ring $\mathbb{Z}_n$, and let $C_i = \{\alpha^{4j+i} : 0 \leqslant j < f\}$, $0 \leqslant i < 4$. Those $C_i, 0 \leqslant i < 4$, are called the cyclotomic classes of order 4 with respect to $\mathbb{Z}_n$. The cyclotomic numbers of order 4, denoted (i, j), are defined as

$$(i, j) = |(C_i + 1) \cap C_j|.$$

The cyclotomic numbers of order 4 are given in Storer's work [1)].

Lemma 2.

• For odd f, the sixteen cyclotomic numbers are given by Table A1, where $A = \frac{n-7+2x}{16}$, $B = \frac{n+1+2x-8y}{16}$, $C = \frac{n+1-6x}{16}$, $D = \frac{n+1+2x+8y}{16}$, $E = \frac{n-3-2x}{16}$.

• For even f, the sixteen cyclotomic numbers are given by Table A2, where $A = \frac{n-11-6x}{16}$, $B = \frac{n-3+2x+8y}{16}$, $C = \frac{n-3+2x}{16}$, $D = \frac{n-3+2x-8y}{16}$, $E = \frac{n+1-2x}{16}$.

Let $s_1, s_2, s_3, s_4, s_5, s_6$ be six binary sequences of odd prime length n with support sets $D_0 \cup D_1$, $D_0 \cup D_2$, $D_0 \cup D_3$, $D_1 \cup D_2$, $D_1 \cup D_3$, $D_2 \cup D_3$, respectively. The auto-correlation and cross-correlation of $s_i, 1 \leqslant i \leqslant 6$, are listed in Tables A3 and A4 respectively.

Let $i_0 i_1 i_2 i_3$ and $j_0 j_1 j_2 j_3$ be two permutations of $0, 1, 2, 3$. Let s_i and s_j be two binary sequences with support sets $D_{i_0} \cup D_{i_1}$ and $D_{j_0} \cup D_{j_1}$, respectively. The cross-correlation of s_i and s_j at shift $\tau \in D_k$ is equal to

$$\begin{aligned} R_{s_i,s_j}(\tau) &= (-1)^{s_i(0)+s_j(\tau)} + (-1)^{s_i(n-\tau)+s_j(0)} + \Delta_{s_i,s_j}(\tau) \\ &= (-1)^{s_j(\tau)} + (-1)^{s_i(n-\tau)} + \Delta_{s_i,s_j}(\tau), \end{aligned} \tag{A1}$$

where

$$\begin{aligned} \Delta_{s_i,s_j}(\tau) = \; & |\{1 \leqslant i < n : i \in D_{i_0}, i+\tau \in D_{j_0}\}| + |\{1 \leqslant i < n : i \in D_{i_0}, i+\tau \in D_{j_1}\}| \\ & -|\{1 \leqslant i < n : i \in D_{i_0}, i+\tau \in D_{j_2}\}| - |\{1 \leqslant i < n : i \in D_{i_0}, i+\tau \in D_{j_3}\}| \\ & +|\{1 \leqslant i < n : i \in D_{i_1}, i+\tau \in D_{j_0}\}| + |\{1 \leqslant i < n : i \in D_{i_1}, i+\tau \in D_{j_1}\}| \\ & -|\{1 \leqslant i < n : i \in D_{i_1}, i+\tau \in D_{j_2}\}| - |\{1 \leqslant i < n : i \in D_{i_1}, i+\tau \in D_{j_3}\}| \\ & -|\{1 \leqslant i < n : i \in D_{i_2}, i+\tau \in D_{j_0}\}| - |\{1 \leqslant i < n : i \in D_{i_2}, i+\tau \in D_{j_1}\}| \\ & +|\{1 \leqslant i < n : i \in D_{i_2}, i+\tau \in D_{j_2}\}| + |\{1 \leqslant i < n : i \in D_{i_2}, i+\tau \in D_{j_3}\}| \\ & -|\{1 \leqslant i < n : i \in D_{i_3}, i+\tau \in D_{j_0}\}| - |\{1 \leqslant i < n : i \in D_{i_3}, i+\tau \in D_{j_1}\}| \\ & +|\{1 \leqslant i < n : i \in D_{i_3}, i+\tau \in D_{j_2}\}| + |\{1 \leqslant i < n : i \in D_{i_3}, i+\tau \in D_{j_3}\}| \\ = \; & (j_0 - k, i_0 - k) + (j_1 - k, i_0 - k) - (j_2 - k, i_0 - k) - (j_3 - k, i_0 - k) \\ & +(j_0 - k, i_1 - k) + (j_1 - k, i_1 - k) - (j_2 - k, i_1 - k) - (j_3 - k, i_1 - k) \\ & -(j_0 - k, i_2 - k) - (j_1 - k, i_2 - k) + (j_2 - k, i_2 - k) + (j_3 - k, i_2 - k) \\ & -(j_0 - k, i_3 - k) - (j_1 - k, i_3 - k) + (j_2 - k, i_3 - k) + (j_3 - k, i_3 - k). \end{aligned} \tag{A2}$$

1) Storer T. Cyclotomy and Difference Sets. Chicago: Markham Publishing Company, 1967.

Table A1 f odd

(i,j)	0	1	2	3
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

Table A2 f even

(i,j)	0	1	2	3
0	A	B	C	D
1	B	D	E	E
2	C	E	C	E
3	D	E	E	B

Lemma 3. For each $1 \leqslant i,j \leqslant 6$, the correlation of s_i and s_j have the following properties:

(1) For any $\tau_1, \tau_2 \in D_k$, $k = 0,1,2,3$, $R_{s_i,s_j}(\tau_1) = R_{s_i,s_j}(\tau_2)$.

(2)

$$R_{s_i,s_j}(0) = \begin{cases} n, & i = j, \\ n-2, & i+j = 7, \\ 1, & \text{otherwise.} \end{cases}$$

(3) For each $\tau \in D_k$ and $l \in D_{k+2}$, where the subscript $k+2$ is performed modulo 4, we have

$$R_{s_i,s_j}(\tau) = \begin{cases} R_{s_j,s_i}(l), & f \text{ odd}, \\ R_{s_j,s_i}(\tau), & f \text{ even}. \end{cases}$$

Proof. The proofs of (1) and (2) are obvious, so we only give the proof of (3). Note that

$$-1 = (-1)^{2f} \in \begin{cases} D_0, & f \text{ odd}, \\ D_2, & f \text{ even}. \end{cases}$$

This implies that $n - \tau \in D_{k+2}$ if f is odd and $n - \tau \in D_k$ if f is even. Hence we have

$$(-1)^{s_i(n-\tau)} = \begin{cases} (-1)^{s_i(l)}, & f \text{ odd}, \\ (-1)^{s_i(\tau)}, & f \text{ even}, \end{cases} \quad \Delta_{s_j,s_i}(n-\tau) = \begin{cases} \Delta_{s_j,s_i}(l), & f \text{ odd}, \\ \Delta_{s_j,s_i}(\tau), & f \text{ even}. \end{cases} \tag{A3}$$

Thus we have

$$\begin{aligned} R_{s_i,s_j}(\tau) &= \sum_{t=0}^{n-1} (-1)^{s_i(t)+s_j(t+\tau)} \\ &= R_{s_j,s_i}(n-\tau) \\ &= (-1)^{s_i(n-\tau)} + (-1)^{s_j(\tau)} + \Delta_{s_j,s_i}(n-\tau) \\ &= \begin{cases} (-1)^{s_i(l)} + (-1)^{s_j(\tau)} + \Delta_{s_j,s_i}(l), & f \text{ odd} \\ (-1)^{s_i(\tau)} + (-1)^{s_j(\tau)} + \Delta_{s_j,s_i}(\tau), & f \text{ even} \end{cases} \\ &= \begin{cases} (-1)^{s_i(l)} + (-1)^{s_j(n-l)} + \Delta_{s_j,s_i}(l), & f \text{ odd} \\ (-1)^{s_i(\tau)} + (-1)^{s_j(n-\tau)} + \Delta_{s_j,s_i}(\tau), & f \text{ even} \end{cases} \\ &= \begin{cases} R_{s_j,s_i}(l), & f \text{ odd}, \\ R_{s_j,s_i}(\tau), & f \text{ even}, \end{cases} \end{aligned}$$

where the third equal sign is due to (A1), and the fourth one is due to (A3).

By (3) of Lemma 3, it is sufficient to consider the correlation of $R_{s_i,s_j}(\tau)$ for $\tau \neq 0$ and $1 \leqslant i \leqslant j \leqslant 6$, which are given in the following two theorems.

Theorem 11. Let f be odd, then the auto- and cross-correlation of $s_1, s_2, s_3, s_4, s_5, s_6$ are given in Table A3.

Proof. We only prove the auto-correlation of s_3, and the remainder results can be similarly discussed. Let $\tau \in D_k$, $k = 0,1,2,3$. By (A2), we have

$$\Delta_{s_3,s_3}(\tau) = (0-k, 0-k) + (3-k, 0-k) - (1-k, 0-k) - (2-k, 0-k)$$

Table A3 The auto- and cross-correlation of six binary sequences of period $n = 4f + 1$, f odd

τ	$\{0\}$	D_0	D_1	D_2	D_3
$R_{s_1}(\tau)$	n	$-2y-1$	$2y-1$	$-2y-1$	$2y-1$
$R_{s_2}(\tau)$	n	-3	1	-3	1
$R_{s_3}(\tau)$	n	$2y-1$	$-2y-1$	$2y-1$	$-2y-1$
$R_{s_4}(\tau)$	n	$2y-1$	$-2y-1$	$2y-1$	$-2y-1$
$R_{s_5}(\tau)$	n	1	-3	1	-3
$R_{s_6}(\tau)$	n	$-2y-1$	$2y-1$	$-2y-1$	$2y-1$
$R_{s_1,s_2}(\tau)$	1	$-x+2y$	$x+2y+2$	$x-2y-2$	$-x-2y$
$R_{s_1,s_3}(\tau)$	1	x	$-x+2$	x	$-x-2$
$R_{s_1,s_4}(\tau)$	1	$-x+2$	x	$-x-2$	x
$R_{s_1,s_5}(\tau)$	1	$x-2y+2$	$-x-2y$	$-x+2y$	$x+2y-2$
$R_{s_1,s_6}(\tau)$	$2-n$	$2y+3$	$3-2y$	$2y-1$	$-1-2y$
$R_{s_2,s_3}(\tau)$	1	$x+2y-2$	$x-2y+2$	$-x-2y$	$-x+2y$
$R_{s_2,s_4}(\tau)$	1	$-x-2y$	$-x+2y$	$x+2y-2$	$x-2y+2$
$R_{s_2,s_5}(\tau)$	$2-n$	1	1	1	1
$R_{s_2,s_6}(\tau)$	1	$2y-x$	$x+2y+2$	$x-2y-2$	$-x-2y$
$R_{s_3,s_4}(\tau)$	$2-n$	$3-2y$	$2y-1$	$-1-2y$	$3+2y$
$R_{s_3,s_5}(\tau)$	1	$x+2y+2$	$x-2y-2$	$-x-2y$	$-x+2y$
$R_{s_3,s_6}(\tau)$	1	$-x+2$	x	$-x-2$	x
$R_{s_4,s_5}(\tau)$	1	$-x-2y$	$-x+2y$	$x+2y+2$	$x-2y-2$
$R_{s_4,s_6}(\tau)$	1	x	$-x+2$	x	$-x-2$
$R_{s_5,s_6}(\tau)$	1	$x-2y+2$	$-x-2y$	$-x+2y$	$x+2y-2$

$$
\begin{aligned}
&+(0-k,3-k)+(3-k,3-k)-(1-k,3-k)-(2-k,3-k)\\
&-(0-k,1-k)-(3-k,1-k)+(1-k,1-k)+(2-k,1-k)\\
&-(0-k,2-k)-(3-k,2-k)+(1-k,2-k)+(2-k,2-k)\\
=&\begin{cases} A-3B-C+D+2E, & k=0,2\\ A+B-C-3D+2E, & k=1,3\end{cases}\\
=&\begin{cases} A-3B-C+D+2E, & \tau\in D_0\cup D_2\\ A+B-C-3D+2E, & \tau\in D_1\cup D_3\end{cases}\\
=&\begin{cases} 2y-1, & \tau\in D_0\cup D_2,\\ -2y-1, & \tau\in D_1\cup D_3,\end{cases}
\end{aligned}
$$

where the second equal sign is due to the cyclotomic numbers given by Table A1 of Lemma 2.

Note that f is odd, $-1=\alpha^{2f}\in D_2$, and we have $(-1)^{s_3(\tau)}+(-1)^{s_3(n-\tau)}=0$ for any $1\leqslant\tau<n$. By (A2) and (A1), the auto-correlation of s_3 is given as follows:

$$
R_{s_3}(\tau)=\begin{cases} 2y-1, & \tau\in D_0\cup D_2,\\ -2y-1, & \tau\in D_1\cup D_3.\end{cases}
$$

Theorem 12. Let f be even, then the auto- and cross-correlation of s_1,s_2,s_3,s_4,s_5,s_6 are given in Table A4.

Proof. We only prove the auto-correlation of s_3, and the remainder results can be similarly discussed. By (A2), we have

$$
\begin{aligned}
\Delta_{s_3,s_3}(\tau)=&(0-k,0-k)+(0-k,3-k)-(0-k,1-k)-(0-k,2-k)\\
&+(3-k,0-k)+(3-k,3-k)-(3-k,1-k)-(3-k,2-k)\\
&-(1-k,0-k)-(1-k,3-k)+(1-k,1-k)+(1-k,2-k)\\
&-(2-k,0-k)-(2-k,3-k)+(2-k,1-k)+(2-k,2-k)\\
=&\begin{cases} A-B-C+3D-2E, & k=0,2\\ A+3B-C-D-2E, & k=1,3\end{cases}\\
=&\begin{cases} -1-2y, & k=0,2\\ -1+2y, & k=1,3\end{cases}
\end{aligned}
$$

Table A4 The auto- and cross-correlation of six binary sequences of period $n = 4f + 1$, f even

τ	$\{0\}$	D_0	D_1	D_2	D_3
$R_{s_1}(\tau)$	n	$2y-3$	$-3-2y$	$1+2y$	$1-2y$
$R_{s_2}(\tau)$	n	-3	1	-3	1
$R_{s_3}(\tau)$	n	$-2y-3$	$2y+1$	$-2y+1$	$2y-3$
$R_{s_4}(\tau)$	n	$-2y+1$	$2y-3$	$-2y-3$	$2y+1$
$R_{s_5}(\tau)$	n	1	-3	1	-3
$R_{s_6}(\tau)$	n	$2y+1$	$-2y+1$	$2y-3$	$-2y-3$
$R_{s_1,s_2}(\tau)$	1	$-x+2y-2$	$x+2y$	$x-2y$	$-x-2y+2$
$R_{s_1,s_3}(\tau)$	1	$-x-2$	x	$-x+2$	x
$R_{s_1,s_4}(\tau)$	1	x	$-x-2$	x	$-x+2$
$R_{s_1,s_5}(\tau)$	1	$x-2y$	$-x-2y-2$	$-x+2y+2$	$x+2y$
$R_{s_1,s_6}(\tau)$	$2-n$	$1-2y$	$1+2y$	$1-2y$	$1+2y$
$R_{s_2,s_3}(\tau)$	1	$-x-2y-2$	$-x+2y+2$	$x+2y$	$x-2y$
$R_{s_2,s_4}(\tau)$	1	$x+2y$	$x-2y$	$-x-2y-2$	$-x+2y+2$
$R_{s_2,s_5}(\tau)$	$2-n$	1	1	1	1
$R_{s_2,s_6}(\tau)$	1	$x-2y$	$-x-2y+2$	$-x+2y-2$	$x+2y$
$R_{s_3,s_4}(\tau)$	$2-n$	$1+2y$	$1-2y$	$1+2y$	$1-2y$
$R_{s_3,s_5}(\tau)$	1	$x+2y$	$x-2y$	$-x-2y+2$	$-x+2y-2$
$R_{s_3,s_6}(\tau)$	1	x	$-x+2$	x	$-x-2$
$R_{s_4,s_5}(\tau)$	1	$-x-2y+2$	$-x+2y-2$	$x+2y$	$x-2y$
$R_{s_4,s_6}(\tau)$	1	$-x+2$	x	$-x-2$	x
$R_{s_5,s_6}(\tau)$	1	$-x+2y+2$	$x+2y$	$x-2y$	$-x-2y-2$

$$= \begin{cases} -1-2y, & \tau \in D_0 \cup D_2, \\ -1+2y, & \tau \in D_1 \cup D_3, \end{cases}$$

where the second equal sign is due to the cyclotomic numbers given by Table A2 of Lemma 2.

Note that f is even, we have $-1 = \alpha^{2f} \in D_0$, and then $n - \tau \in D_k$ for $\tau \in D_k$. Hence one has

$$(-1)^{s_3(\tau)} + (-1)^{s_3(n-\tau)} = \begin{cases} -2, & \tau \in D_0 \cup D_3, \\ 2, & \tau \in D_1 \cup D_2. \end{cases}$$

By (A2) and (A1), the auto-correlation of s_3 is given as follows:

$$R_{s_3}(\tau) = \begin{cases} -3-2y, & \tau \in D_0, \\ 1+2y, & \tau \in D_1, \\ 1-2y, & \tau \in D_2, \\ -3+2y, & \tau \in D_3. \end{cases}$$