

TWO CLASSES OF BINARY SEQUENCES OF PERIOD $4p$ WITH LOW AUTOCORRELATION AND LARGE LINEAR COMPLEXITY

YANG Bo, ZHU Zi-kun, XIAO Zi-bi

(College of Science, Wuhan University of Science and Technology, Wuhan 430065, China)

Abstract: The design of binary sequences with good autocorrelation property and large linear complexity is very important for diverse applications of communication systems and stream ciphers. In this paper, we propose two classes of binary sequences of period $4p$ constructed by interleaving four appropriate sequences chosen from Hall's sextic residue sequences and their modified versions. The autocorrelation and linear complexity of these sequences are completely determined. The results show that the proposed sequences have both low autocorrelation sidelobes as well as very large linear complexity.

Keywords: binary sequences; interleaved structure; autocorrelation; linear complexity

2010 MR Subject Classification: 11T22; 11T55; 94A55; 94A60

Document code: A **Article ID:** 0255-7797(2024)01-0017-18

1 Introduction

Binary sequences with good autocorrelation property and large linear complexity are widely used in many areas of communication systems and cryptography [1–4]. The (periodic) cross-correlation function of two binary sequences $a = (a(0), a(1), \dots, a(N-1))$ and $b = (b(0), b(1), \dots, b(N-1))$ of period N at shift τ is defined by

$$R_{a,b}(\tau) = \sum_{t=0}^{N-1} (-1)^{a(t)+b(t+\tau)}, \quad 0 \leq \tau < N,$$

where the sum $t + \tau$ is computed modulo N . When the two sequences a and b are identical, the cross-correlation function is called the autocorrelation function of a , and is denoted by $R_a(\tau)$. The values of $R_a(\tau)$, $1 \leq \tau < N$, are called the out-of-phase autocorrelation values of a .

Let $a = (a(0), a(1), \dots, a(N-1))$ be a binary sequence of period N and $\mathbb{Z}_N = \{0, 1, \dots, N-1\}$ denote the ring of integers modulo N . The subset C of \mathbb{Z}_N is called the support set of a sequence a if

$$a(i) = \begin{cases} 1, & i \pmod{N} \in C, \\ 0, & \text{otherwise.} \end{cases}$$

* Received date: 2022-10-30

Accepted date: 2022-12-15

Foundation item: Supported by National Natural Science Foundation of China (12061027).

Biography: Yang Bo(1973–), male, born at Xiaogan, Hubei, associate professor, major in sequence design and cryptography. E-mail: yangbo@wust.edu.cn.

It is well known that $R_a(\tau) = N - 4(|C| - |(C + \tau) \cap C|)$, where $C + \tau = \{x + \tau : x \in C\}$ [5]. Clearly, $R_a(\tau) \equiv N \pmod{4}$. According to the remainder of N modulo 4, the optimal out-of-phase autocorrelation values of binary sequences in terms of the smallest possible values of the autocorrelation are classified into four types as follows [6]:

- (A) $R_a(\tau) = 0$ if $N \equiv 0 \pmod{4}$;
- (B) $R_a(\tau) = -1$ if $N \equiv 3 \pmod{4}$;
- (C) $R_a(\tau) \in \{1, -3\}$ if $N \equiv 1 \pmod{4}$;
- (D) $R_a(\tau) \in \{2, -2\}$ if $N \equiv 2 \pmod{4}$.

In particular, if a sequence has out-of-phase autocorrelation of type (B), it is often called an ideal sequence. If a sequence has out-of-phase autocorrelation of type (A), it is referred to as a perfect sequence. Unfortunately, the only known perfect binary sequence up to equivalence (shift and complement) is $(0, 0, 0, 1)$. It is conjectured that there is no perfect binary sequence of period N greater than 4 [7]. Therefore, a binary sequence a of period $N \equiv 0 \pmod{4}$ is referred to as a sequence with optimal autocorrelation value if its out-of-phase autocorrelation values $R_a(\tau) \in \{0, 4\}$ or $R_a(\tau) \in \{0, -4\}$, and is referred to as a sequence with optimal autocorrelation magnitude if its out-of-phase autocorrelation values $R_a(\tau) \in \{0, 4, -4\}$ [6, 8].

Linear complexity of a sequence is defined as the length of the shortest linear feedback shift registers that can generate the sequence. If the linear complexity of a sequence is l , then the famous Berlekamp-Massey algorithm [9] can recover the whole sequence from $2l$ consecutive digits of the sequence. Therefore, large linear complexity of sequences is required for cryptographic applications.

An important method used to construct sequences of period $N \equiv 0 \pmod{4}$ is interleaving technique, which was introduced in [10] for constructing new sequences of an interleaved form from base sequences with good autocorrelation. In 2008, Yu and Gong [8] presented $4 \times (2^m - 1)$ interleaved sequences with optimal autocorrelation magnitude for which all $2^m - 1$ base sequences are shift equivalent to the perfect binary sequence, and derived the exact linear complexity of the sequences. Yu and Gong [8] also showed that the ADS sequences proposed in [11] are $N \times 4$ interleaved sequences for which all four base sequences are shift equivalent up to the complement. Tang and Ding [12] generalized the ADS sequences by using two arbitrary ideal sequences and their shifted sequences as base sequences and got more sequences with optimal autocorrelation values. Xiong et al. [13] presented a sufficient condition and a necessary condition for the linear complexity of these sequences to attain their maximums. In [6], Tang and Gong proposed a $N \times 4$ interleaved structure

$$w = I(a_0 + b(0), L^{d+\eta}(a_1) + b(1), L^{2d}(a_2) + b(2), L^{3d+\eta}(a_3) + b(3)), \quad (1.1)$$

where d is some integer such that $4d \equiv 1 \pmod{p}$, I and L denote the interleaving operator and the left cyclic shift operator, respectively (see definition in Section 2.1), $(b(0), b(1), b(2), b(3))$ is a binary perfect sequence. Based on this interleaved structure, they gave three new constructions of sequences with optimal autocorrelation value/magnitude by choosing different

three pairs of related sequences as base sequences. The linear complexity of these sequences was discussed in [14]. In 2018, Su et al. [15] modified the structure (1.1) and presented a construction of binary sequences with optimal autocorrelation magnitude by choosing base sequences from four suitable Ding-Helleseth-Lam sequences [16]. Soon after, Fan [17] determined the linear complexity of these sequences.

In this paper, two classes of binary interleaved sequences of period $4p$ with low autocorrelation and large linear complexity are constructed by using the interleaved structure (1.1). Different from the previous ones in [6, 11, 15], we extend the requirement for the number and autocorrelation properties of base sequences and choose four base sequences from Hall's sextic residue sequences and their modifications (see Section 2.2). The out-of-phase autocorrelation values of the two classes of binary sequences are $\{0, \pm 4, \pm 8\}$ and $\{0, \pm 4, -8\}$ respectively, which are the closest to optimal autocorrelation magnitude. In order to determine the linear complexity of the constructed sequences, we adopt the classical approach described in [18, 19] and focus on the investigation of the roots of corresponding sequence polynomials in the splitting field of $x^p - 1$ over the finite field \mathbb{F}_2 . As a consequence, both the minimal polynomial and linear complexity of these two classes of interleaved sequences are determined. The linear complexity of the second class of sequences is equal to $4p - \gamma$ with $\gamma \in \{1, 2, 3, 4\}$. In most cases the linear complexity of the first class of sequences is equal to $4p$. Our results show that their linear complexity is quite good.

The remainder of this paper is organized as follows. Section 2 gives some preliminaries. In Section 3, we present two classes of binary interleaved sequences of period $4p$ and compute their out-of-phase autocorrelation values. The linear complexity of the proposed sequences is determined in Section 4. Section 5 concludes this paper.

2 Preliminaries

In this section, we introduce some basic concepts and related results required for the construction of new sequences and the determination of their autocorrelation and linear complexity.

2.1 Interleaved Structure

Given a family $\{a_0, a_1, \dots, a_{M-1}\}$ of M sequences of period N , where sequences $a_i = (a_i(0), a_i(1), \dots, a_i(N-1))$, $0 \leq i < M$. An $N \times M$ matrix U is formed by placing the sequences a_i on the i th column, where $0 \leq i < M$. Then one can obtain an interleaved sequence u of period NM by concatenating the successive rows of the matrix U . For simplicity, the interleaved sequence u can be written as $u = I(a_0, a_1, \dots, a_{M-1})$, where I denotes the interleaving operator and a_i with $0 \leq i < M$ are called the base sequences of u .

Let L be the cyclic left shift operator of a sequence $a = (a(0), a(1), \dots, a(N-1))$ of period N , which is defined by $L(a) = (a(1), a(2), \dots, a(N-1), a(0))$. Then the cyclic left shift τ bits of a can be represented as $L^\tau(a) = (a(\tau), a(\tau+1), \dots, a(N-1), a(0), \dots, a(\tau-1))$.

The following lemma shows that the cyclic left shift and autocorrelation function of an

interleaved sequence $s = I(a_0, a_1, \dots, a_{M-1})$ can be expressed in terms of the cyclic left shift and cross-correlation function of its base sequences, respectively.

Lemma 2.1 (see [6]) Let $s = I(a_0, a_1, \dots, a_{M-1})$ be the interleaved sequence from the base sequences a_i , $0 \leq i < M$, of period N . Then

(i) the cyclic left shift τ bits of s is given by

$$L^\tau(s) = I(L^{\tau_1}(a_{\tau_2}), \dots, L^{\tau_1}(a_{M-1}), L^{\tau_1+1}(a_0), \dots, L^{\tau_1+1}(a_{\tau_2-1})),$$

(ii) the autocorrelation function of s at shift τ is given by

$$R_s(\tau) = \sum_{i=0}^{M-\tau_2-1} R_{a_i, a_{i+\tau_2}}(\tau_1) + \sum_{i=M-\tau_2}^{M-1} R_{a_i, a_{i+\tau_2-M}}(\tau_1 + 1),$$

where $\tau = \tau_1 M + \tau_2$ ($0 \leq \tau_1 < N$, $0 \leq \tau_2 < M$).

2.2 Hall's Sextic Residue Sequences and Their Modifications

Let $p = 6f + 1$ be an odd prime, where f is a positive integer. Let g be a primitive root modulo p . Define

$$D_i = \{g^{6j+i} : 0 \leq j < f\}, \quad i = 0, 1, \dots, 5.$$

These D_i , $i = 0, 1, \dots, 5$, are called cyclotomic classes of order 6 with respect to p [20].

Lemma 2.2 Let $p = 6f + 1$ be an odd prime. Then

(i) (see [20]) $-1 \in D_3$ if f is odd;

(ii) (see [1]) For $a \in D_j$ with $0 \leq j < 6$, we have $aD_i = D_{(i+j) \pmod{6}}$.

Put $C_i = D_i \cup D_{i+1} \cup D_{i+3}$ with $i \in \{0, 1, \dots, 5\}$, where all indices are calculated modulo 6, and assume that s_i with $i \in \{0, 1, \dots, 5\}$ are binary sequences of period p with support sets C_i . It has been shown that if the prime $p = 6f + 1$ is of the form $4A + 27$ and g is chosen such that $3 \in D_1$, then each C_i forms a cyclic difference set [21]. This implies that the sequences s_i with $i \in \{0, 1, \dots, 5\}$ are all ideal sequences. These six sequences are called Hall's sextic residue sequences.

For each Hall's sextic residue sequence s_i , by replacing the first bit 0 in s_i with 1, we obtain the corresponding modified version s'_i of s_i with period p , which is defined by

$$s'_i(t) = \begin{cases} 1, & \text{if } t \equiv 0 \pmod{p}, \\ s_i(t), & \text{otherwise.} \end{cases} \quad (2.1)$$

We shall henceforth use s_i and s'_i with $i \in \{0, 1, 2, \dots, 5\}$ to denote Hall's sextic residue sequences of period p and their corresponding modifications. The following lemma gives several correlation properties of s_i and s'_i that we shall need later.

Lemma 2.3 Let $0 \leq \tau < p$ and $0 \leq i, j \leq 5$. Then we have

(i) the autocorrelation of s'_i is given by

$$R_{s'_i}(\tau) = \begin{cases} p, & \text{if } \tau = 0, \\ -1 - 2((-1)^{s_i(\tau)} + (-1)^{s_i(-\tau)}), & \text{otherwise;} \end{cases}$$

(ii) the cross-correlation between s_i and s'_j is given by

$$R_{s_i, s'_j}(\tau) = R_{s_i, s_j}(\tau) - 2(-1)^{s_i(-\tau)};$$

(iii) the cross-correlation between s'_i and s_j is given by

$$R_{s'_i, s_j}(\tau) = R_{s_i, s_j}(\tau) - 2(-1)^{s_j(\tau)};$$

(iv) the cross-correlation between s'_i and s'_j is given by

$$R_{s'_i, s'_j}(\tau) = \begin{cases} R_{s_i, s_j}(0), & \text{if } \tau = 0, \\ R_{s_i, s_j}(\tau) - 2((-1)^{s_j(\tau)} + (-1)^{s_i(-\tau)}), & \text{otherwise.} \end{cases}$$

Proof We prove only (iv) and the others can be proved similarly. If $\tau = 0$, we have

$$\begin{aligned} R_{s'_i, s'_j}(0) &= \sum_{t=0}^{p-1} (-1)^{s'_i(t) + s'_j(t)} \\ &= \sum_{t=0}^{p-1} (-1)^{s_i(t) + s_j(t)} + (-1)^{s'_i(0) + s'_j(0)} - (-1)^{s_i(0) + s_j(0)} \\ &= \sum_{t=0}^{p-1} (-1)^{s_i(t) + s_j(t)} = R_{s_i, s_j}(0). \end{aligned}$$

If $\tau \neq 0$, we have

$$\begin{aligned} R_{s'_i, s'_j}(\tau) &= \sum_{t=0}^{p-1} (-1)^{s'_i(t) + s'_j(t+\tau)} \\ &= \sum_{t=0}^{p-1} (-1)^{s_i(t) + s_j(t+\tau)} + (-1)^{s'_i(0) + s'_j(\tau)} + (-1)^{s'_i(-\tau) + s'_j(0)} \\ &\quad - (-1)^{s_i(0) + s_j(\tau)} - (-1)^{s_i(-\tau) + s_j(0)} \\ &= R_{s_i, s_j}(\tau) - (-1)^{s'_j(\tau)} - (-1)^{s'_i(-\tau)} - (-1)^{s_j(\tau)} - (-1)^{s_i(-\tau)} \\ &= R_{s_i, s_j}(\tau) - 2((-1)^{s_j(\tau)} + (-1)^{s_i(-\tau)}). \end{aligned}$$

2.3 Sequence Polynomial and Linear Complexity

We first point out that throughout this paper we study binary sequences. Hence, all the polynomials are in $\mathbb{F}_2[x]$, where $\mathbb{F}_2[x]$ denotes the set of all the polynomials in x over \mathbb{F}_2 .

Let $s = (s(0), s(1), \dots, s(N-1))$ be a binary sequence of period N . The linear complexity $LC(s)$ of s is the smallest positive integer l for which there exist constants $c_0 = 1, c_1, c_2, \dots, c_l \in \mathbb{F}_2$ such that $s(i) + c_1s(i-1) + c_2s(i-2) + \dots + c_ls(i-l) = 0$ holds for all $i \geq l$. Equivalently, $LC(s)$ is the degree of the polynomial $m_s(x) = 1 + c_1x + \dots + c_lx^l$. The polynomial $m_s(x)$ is called the minimal polynomial of s .

Let $P_s(x) = s(0) + s(1)x + \cdots + s(N-1)x^{N-1}$ be the sequence polynomial of a binary sequence s of period N . Then the minimal polynomial and linear complexity of s can be calculated by using the following lemma.

Lemma 2.4 (see [22]) For a binary sequence s of period N ,

- (i) the minimal polynomial of s is given by $m_s(x) = \frac{x^N - 1}{\gcd(x^N - 1, P_s(x))}$;
- (ii) the linear complexity of s is given by $LC(s) = N - \deg(\gcd(x^N - 1, P_s(x)))$,

where $\deg(f(x))$ denotes the degree of the polynomial $f(x)$ and $\gcd(g(x), h(x))$ denotes the greatest common divisor of the polynomials $g(x)$ and $h(x)$.

The following lemma gives the relations of sequence polynomials of some related sequences.

Lemma 2.5 (see [14, 23]) Let a_0, a_1, a_2, a_3 be binary sequences of period N . Then

- (i) $P_{b_0}(x) = x^{N-\tau} P_{a_0}(x)$ if $b_0 = L^\tau(a_0)$;
- (ii) $P_{b_0}(x) = P_{a_0}(x) + \frac{x^N - 1}{x - 1}$ if b_0 is the complement sequence of a_0 (i.e., $b_0(t) = a_0(t) + 1$);
- (iii) $P_w(x) = P_{a_0}(x^4) + x P_{a_1}(x^4) + x^2 P_{a_2}(x^4) + x^3 P_{a_3}(x^4)$ if $w = I(a_0, a_1, a_2, a_3)$.

For Hall's sextic residue sequences and their modifications, we have the following facts.

Lemma 2.6 Let s_i and s'_i , $0 \leq i \leq 5$ be Hall's sextic residue sequences and their modifications defined by (2.1). Then

- (i) $P_{s'_i}(x) = P_{s_i}(x) + 1$;
- (ii) $P_{s_i}(x^4) \equiv 1 \pmod{x^4 - 1}$.

Proof (i) is obvious, so we only prove (ii). Note that $x^{4k} \equiv 1 \pmod{x^4 - 1}$ for any positive integer k . Then from the definition of Hall's sextic residue sequence s_i with period p , we get

$$P_{s_i}(x^4) = \sum_{k \in C_i} x^{4k} \equiv \frac{p-1}{2} \pmod{x^4 - 1}.$$

Since p is of the form $4A + 27$, it follows that $\frac{p-1}{2}$ is an odd number, which yields the desired result.

3 Two Classes of Binary Sequences and Their Autocorrelations

In this section, we construct two classes of binary sequences of period $4p$ with low autocorrelation by interleaving four appropriate base sequences selected from Hall's sextic residue sequences and their modifications.

3.1 The First Class

Let s_i and s_j be two Hall's sextic residue sequences of period p , where the integers i, j satisfy $0 \leq i, j \leq 5$ and $j - i \not\equiv 0 \pmod{3}$. Let $b = (b(0), b(1), b(2), b(3))$ be a perfect binary sequence. Define the first class of binary sequences u of period $4p$ as

$$u = I(s_i + b(0), L^{d+\eta}(s_j) + b(1), L^{2d}(s'_i) + b(2), L^{3d+\eta}(s'_j) + b(3)), \quad (3.1)$$

where d is some integer such that $4d \equiv 1 \pmod{p}$, η is an integer such that $0 \leq \eta < p$.

Theorem 3.1 The first class of binary sequences u defined by (3.1) has $R_u(\tau) \in \{0, \pm 4, \pm 8\}$ for all $1 \leq \tau < 4p$.

Proof Writing $\tau = 4\tau_1 + \tau_2$, where $0 \leq \tau_1 < p$ and $0 < \tau_2 < 4$ or $0 < \tau_1 < p$ and $\tau_2 = 0$, we calculate the out-of-phase autocorrelation values of the sequence u in four cases.

Case 1. $\tau_2 = 0$, $0 < \tau_1 < p$. In this case, one has

$$L^\tau(u) = I(L^{\tau_1}(s_i) + b(0), L^{\tau_1+d+\eta}(s_j) + b(1), L^{\tau_1+2d}(s'_i) + b(2), L^{\tau_1+3d+\eta}(s'_j) + b(3))$$

by Lemma 2.1(i). Then applying the ideal autocorrelation property of Hall's sextic residue sequences and Lemmas 2.1(ii) and 2.3(i) we get that the autocorrelation of u at shift $\tau = 4\tau_1$ which is

$$\begin{aligned} R_u(\tau) &= R_{s_i}(\tau_1) + R_{s_j}(\tau_1) + R_{s'_i}(\tau_1) + R_{s'_j}(\tau_1) \\ &= (-1) + (-1) + (-1) - 2((-1)^{s_i(\tau_1)} + (-1)^{s_i(-\tau_1)}) \\ &\quad + (-1) - 2((-1)^{s_j(\tau_1)} + (-1)^{s_j(-\tau_1)}) \\ &= -4 - 2H_{i,j}(\tau_1), \end{aligned} \tag{3.2}$$

where $H_{i,j}(\tau_1) = (-1)^{s_i(\tau_1)} + (-1)^{s_i(-\tau_1)} + (-1)^{s_j(\tau_1)} + (-1)^{s_j(-\tau_1)}$. Since the period $p = 6f + 1$ of any Hall's sextic residue sequence is a prime of the form $4A + 27$, $f = \frac{p-1}{6}$ is an odd number, and it follows from Lemma 2.2(i) that $-1 \in D_3$. Then, according to the definition of Hall's sextic residue sequence and Lemma 2.2(ii), the values of $H_{i,j}(\tau_1)$, $0 \leq i, j \leq 5$ can be obtained by straightforward calculations, which we list in Table 1.

Table 1 Values of $H_{i,j}(\tau_1)$

τ_1	$D_i \cup D_{i+3}$	$D_{i+1} \cup D_{i+4}$	$D_{i+2} \cup D_{i+5}$
$H_{i,j}(\tau_1), j - i \equiv 1 \pmod{3}$	0	-2	2
$H_{i,j}(\tau_1), j - i \equiv 2 \pmod{3}$	-2	2	0

Substituting the value of $H_{i,j}(\tau_1)$ into (3.2), we get

$$R_u(\tau) = \begin{cases} -4, & \tau_1 \in D_i \cup D_{i+3}, \\ 0, & \tau_1 \in D_{i+1} \cup D_{i+4}, \\ -8, & \tau_1 \in D_{i+2} \cup D_{i+5}, \end{cases}$$

if $j - i \equiv 1 \pmod{3}$, and

$$R_u(\tau) = \begin{cases} 0, & \tau_1 \in D_i \cup D_{i+3}, \\ -8, & \tau_1 \in D_{i+1} \cup D_{i+4}, \\ -4, & \tau_1 \in D_{i+2} \cup D_{i+5}, \end{cases}$$

if $j - i \equiv 2 \pmod{3}$.

Case 2. $\tau_2 = 1$, $0 \leq \tau_1 < p$. In this case, one has

$$L^\tau(u) = I(L^{\tau_1+d+\eta}(s_j) + b(1), L^{\tau_1+2d}(s'_i) + b(2), L^{\tau_1+3d+\eta}(s'_j) + b(3), L^{\tau_1+1}(s_i) + b(0))$$

by Lemma 2.1(i). Then by Lemma 2.1(ii) the autocorrelation of u at shift $\tau = 4\tau_1 + 1$ is given by

$$\begin{aligned} R_u(\tau) &= (-1)^{b(0)+b(1)} R_{s_i, s_j}(\tau_1 + d + \eta) + (-1)^{b(1)+b(2)} R_{s_j, s'_i}(\tau_1 + d - \eta) \\ &\quad + (-1)^{b(2)+b(3)} R_{s'_i, s'_j}(\tau_1 + d + \eta) + (-1)^{b(3)+b(0)} R_{s'_j, s_i}(\tau_1 + 1 - 3d - \eta) \\ &= (-1)^{b(0)+b(1)} \left(R_{s_i, s_j}(\tau_1 + d + \eta) - R_{s'_i, s'_j}(\tau_1 + d + \eta) \right) \\ &\quad + (-1)^{b(1)+b(2)} \left(R_{s_j, s'_i}(\tau_1 + d - \eta) - R_{s'_j, s_i}(\tau_1 + d - \eta) \right). \end{aligned}$$

The last identity holds since $b(0) + b(1) + b(2) + b(3) \equiv 1 \pmod{2}$ and $1 - 3d \equiv d \pmod{p}$.

If $\tau_1 \not\equiv -d - \eta \pmod{p}$, then from Lemma 2.3(ii)(iii)(iv) we get

$$\begin{aligned} R_u(\tau) &= 2(-1)^{b(0)+b(1)} \left((-1)^{s_j(\tau_1+d+\eta)} + (-1)^{s_i(-(\tau_1+d+\eta))} \right) \\ &\quad + 2(-1)^{b(1)+b(2)} \left((-1)^{s_i(\tau_1+d-\eta)} - (-1)^{s_j(-(\tau_1+d-\eta))} \right). \end{aligned}$$

Since the values of $(-1)^{s_j(\tau_1+d+\eta)} + (-1)^{s_i(-(\tau_1+d+\eta))}$ and $(-1)^{s_i(\tau_1+d-\eta)} - (-1)^{s_j(-(\tau_1+d-\eta))}$ both belong to $\{0, \pm 2\}$, it follows that $R_u(\tau) \in \{0, \pm 4, \pm 8\}$.

If $\tau_1 \equiv -d - \eta \pmod{p}$, then also by Lemma 2.3(ii)(iii)(iv) we get

$$R_u(\tau) = 2(-1)^{b(1)+b(2)} \left((-1)^{s_i(\tau_1+d-\eta)} - (-1)^{s_j(-(\tau_1+d-\eta))} \right),$$

which clearly belongs to $\{0, \pm 4\}$.

Case 3. $\tau_2 = 2$, $0 \leq \tau_1 < p$. In this case, one has

$$L^\tau(u) = I(L^{\tau_1+2d}(s'_i) + b(2), L^{\tau_1+3d+\eta}(s'_j) + b(3), L^{\tau_1+1}(s_i) + b(0), L^{\tau_1+d+\eta+1}(s_j) + b(1))$$

by Lemma 2.1(i). Then by Lemmas 2.1(ii) and 2.3(ii)(iii) the autocorrelation of u at shift $\tau = 4\tau_1 + 2$ is given by

$$\begin{aligned} R_u(\tau) &= (-1)^{b(0)+b(2)} R_{s_i, s'_i}(\tau_1 + 2d) + (-1)^{b(1)+b(3)} R_{s_j, s'_j}(\tau_1 + 2d) \\ &\quad + (-1)^{b(2)+b(0)} R_{s'_i, s_i}(\tau_1 + 1 - 2d) + (-1)^{b(3)+b(1)} R_{s'_j, s_j}(\tau_1 + 1 - 2d) \\ &= (-1)^{b(0)+b(2)} \left(R_{s_i, s'_i}(\tau_1 + 2d) + R_{s'_i, s_i}(\tau_1 + 2d) \right) \\ &\quad + (-1)^{b(1)+b(3)} \left(R_{s_j, s'_j}(\tau_1 + 2d) + R_{s'_j, s_j}(\tau_1 + 2d) \right) \\ &= (-1)^{b(0)+b(2)} \left(R_{s_i, s'_i}(\tau_1 + 2d) + R_{s'_i, s_i}(\tau_1 + 2d) - R_{s_j, s'_j}(\tau_1 + 2d) - R_{s'_j, s_j}(\tau_1 + 2d) \right) \\ &= (-1)^{b(0)+b(2)} \left(R_{s_i}(\tau_1 + 2d) - 2(-1)^{s_i(-(\tau_1+2d))} + R_{s_i}(\tau_1 + 2d) - 2(-1)^{s_i(\tau_1+2d)} \right. \\ &\quad \left. - R_{s_j}(\tau_1 + 2d) + 2(-1)^{s_j(-(\tau_1+2d))} - R_{s_j}(\tau_1 + 2d) + 2(-1)^{s_j(\tau_1+2d)} \right) \\ &= 2(-1)^{b(0)+b(2)} M_{i,j}(\tau_1 + 2d), \end{aligned}$$

where $M_{i,j}(\tau_1 + 2d) = -(-1)^{s_i(-(\tau_1+2d))} - (-1)^{s_i(\tau_1+2d)} + (-1)^{s_j(-(\tau_1+2d))} + (-1)^{s_j(\tau_1+2d)}$, the second identity holds since $1 - 2d \equiv 2d \pmod{p}$, and the third identity holds since $b(0) + b(1) + b(2) + b(3) \equiv 1 \pmod{2}$. By the definition of Hall's sextic residue sequence s_i and Lemma 2.2, the values of $M_{i,j}(\tau_1 + 2d)$, $0 \leq i, j \leq 5$, are given in Table 2.

Table 2 Values of $M_{i,j}(\tau_1 + 2d)$

$(\tau_1 + 2d) \pmod{p}$	0	$D_i \cup D_{i+3}$	$D_{i+1} \cup D_{i+4}$	$D_{i+2} \cup D_{i+5}$
$M_{i,j}(\tau_1 + 2d), j - i \equiv 1 \pmod{3}$	0	4	-2	-2
$M_{i,j}(\tau_1 + 2d), j - i \equiv 2 \pmod{3}$	0	2	2	-4

If $j - i \equiv 1 \pmod{3}$, the out-of-phase autocorrelation distribution of the sequence u is

$$R_u(\tau) = \begin{cases} 0, & (\tau_1 + 2d) \equiv 0 \pmod{p}, \\ 8(-1)^{b(0)+b(2)}, & (\tau_1 + 2d) \pmod{p} \in D_i \cup D_{i+3}, \\ -4(-1)^{b(0)+b(2)}, & (\tau_1 + 2d) \pmod{p} \in D_{i+1} \cup D_{i+4} \cup D_{i+2} \cup D_{i+5}. \end{cases}$$

If $j - i \equiv 2 \pmod{3}$, the out-of-phase autocorrelation distribution of the sequence u is

$$R_u(\tau) = \begin{cases} 0, & (\tau_1 + 2d) \equiv 0 \pmod{p}, \\ 4(-1)^{b(0)+b(2)}, & (\tau_1 + 2d) \pmod{p} \in D_i \cup D_{i+3} \cup D_{i+1} \cup D_{i+4}, \\ -8(-1)^{b(0)+b(2)}, & (\tau_1 + 2d) \pmod{p} \in D_{i+2} \cup D_{i+5}. \end{cases}$$

Case 4. $\tau_2 = 3$, $0 \leq \tau_1 < p$. In this case, one has

$$L^\tau(u) = I(L^{\tau_1+3d+\eta}(s'_j) + b(3), L^{\tau_1+1}(s_i) + b(0), L^{\tau_1+d+\eta+1}(s_j) + b(1), L^{\tau_1+2d+1}(s'_i) + b(2))$$

by Lemma 2.1(i). Then by Lemma 2.1(ii) the autocorrelation of u at shift $\tau = 4\tau_1 + 3$ is given by

$$\begin{aligned} R_u(\tau) &= (-1)^{b(0)+b(3)} R_{s_i, s'_j}(\tau_1 + 3d + \eta) + (-1)^{b(1)+b(0)} R_{s_j, s_i}(\tau_1 + 1 - d - \eta) \\ &\quad + (-1)^{b(2)+b(1)} R_{s'_i, s_j}(\tau_1 + 1 - d + \eta) + (-1)^{b(3)+b(2)} R_{s'_j, s'_i}(\tau_1 + 1 - d - \eta) \\ &= (-1)^{b(0)+b(3)} R_{s_i, s'_j}(\tau_1 + 3d + \eta) + (-1)^{b(1)+b(0)} R_{s_j, s_i}(\tau_1 + 3d - \eta) \\ &\quad + (-1)^{b(2)+b(1)} R_{s'_i, s_j}(\tau_1 + 3d + \eta) + (-1)^{b(3)+b(2)} R_{s'_j, s'_i}(\tau_1 + 3d - \eta) \\ &= (-1)^{b(0)+b(3)} \left(R_{s_i, s'_j}(\tau_1 + 3d + \eta) - R_{s'_i, s_j}(\tau_1 + 3d + \eta) \right) \\ &\quad + (-1)^{b(0)+b(1)} \left(R_{s_j, s_i}(\tau_1 + 3d - \eta) - R_{s'_j, s'_i}(\tau_1 + 3d - \eta) \right). \end{aligned}$$

The second identity holds since $1 - d \equiv 3d \pmod{p}$, and the last identity holds since $b(0) + b(1) + b(2) + b(3) \equiv 1 \pmod{2}$.

If $\tau_1 \not\equiv -3d + \eta \pmod{p}$, then from Lemma 2.3(ii)(iii)(iv) we get

$$\begin{aligned} R_u(\tau) &= 2(-1)^{b(0)+b(3)} \left(-(-1)^{s_i(-\tau_1+3d+\eta)} + (-1)^{s_j(\tau_1+3d+\eta)} \right) \\ &\quad + 2(-1)^{b(0)+b(1)} \left((-1)^{s_i(\tau_1+3d-\eta)} + (-1)^{s_j(-\tau_1+3d-\eta)} \right). \end{aligned}$$

Since the values of $-(-1)^{s_i(-\tau_1+3d+\eta)} + (-1)^{s_j(\tau_1+3d+\eta)}$ and $(-1)^{s_i(\tau_1+3d-\eta)} + (-1)^{s_j(-\tau_1+3d-\eta)}$ belong to $\{0, \pm 2\}$, it follows that $R_u(\tau) \in \{0, \pm 4, \pm 8\}$.

If $\tau_1 \equiv -3d + \eta \pmod{p}$, then also by Lemma 2.3(ii)(iii)(iv) we get

$$R_u(\tau) = 2(-1)^{b(0)+b(3)} \left(-(-1)^{s_i(-\tau_1+3d+\eta)} + (-1)^{s_j(\tau_1+3d+\eta)} \right),$$

which belongs to $\{0, \pm 4\}$.

Summarizing the results in all cases, we have $R_u(\tau) \in \{0, \pm 4, \pm 8\}$. The proof of this theorem is complete.

3.2 The Second Class

Let s_i and s_j be two Hall's sextic residue sequences of period p with $0 \leq i, j \leq 5$, and $b = (b(0), b(1), b(2), b(3))$ be a perfect binary sequence. Define the second class of binary sequences v of period $4p$ as

$$v = I(s_i + b(0), L^{d+\eta}(s_j) + b(1), L^{2d}(s_i) + b(2), L^{3d+\eta}(s'_j) + b(3)), \quad (3.3)$$

where d is some integer such that $4d \equiv 1 \pmod{p}$, η is an integer such that $0 \leq \eta < p$.

Theorem 3.2 Let v be a binary sequence of period $4p$ defined by (3.3). Then $R_v(\tau) \in \{0, \pm 4, -8\}$ for all $1 \leq \tau < 4p$.

Proof Writing $\tau = 4\tau_1 + \tau_2$, where $0 \leq \tau_1 < p$ and $0 < \tau_2 < 4$ or $0 < \tau_1 < p$ and $\tau_2 = 0$. Applying Lemmas 2.1 and 2.3, the out-of-phase autocorrelation values of v can be calculated in four cases.

Case 1. $\tau_2 = 0, 0 < \tau_1 < p$. In this case, one has

$$L^\tau(v) = I(L^{\tau_1}(s_i) + b(0), L^{\tau_1+d+\eta}(s_j) + b(1), L^{\tau_1+2d}(s_i) + b(2), L^{\tau_1+3d+\eta}(s'_j) + b(3)).$$

Then the autocorrelation of v at shift $\tau = 4\tau_1$ is

$$\begin{aligned} R_v(\tau) &= R_{s_i}(\tau_1) + R_{s_j}(\tau_1) + R_{s_i}(\tau_1) + R_{s'_j}(\tau_1) \\ &= R_{s_i}(\tau_1) + R_{s_j}(\tau_1) + R_{s_i}(\tau_1) + R_{s_j}(\tau_1) - 2((-1)^{s_j(\tau_1)} + (-1)^{s_j(-\tau_1)}) \\ &= -4 - 2A_j(\tau_1), \end{aligned}$$

where

$$A_j(\tau_1) = (-1)^{s_j(\tau_1)} + (-1)^{s_j(-\tau_1)}. \quad (3.4)$$

By the definition of Hall's sextic residue sequence s_j and Lemma 2.2, we have

$$A_j(\tau_1) = \begin{cases} -2, & \tau_1 \in D_j \cup D_{j+3}, \\ 0, & \tau_1 \in D_{j+1} \cup D_{j+4}, \\ 2, & \tau_1 \in D_{j+2} \cup D_{j+5}. \end{cases} \quad (3.5)$$

Hence, the out-of-phase autocorrelation distribution of the sequence v is

$$R_v(\tau) = \begin{cases} 0, & \tau_1 \in D_j \cup D_{j+3}, \\ -4, & \tau_1 \in D_{j+1} \cup D_{j+4}, \\ -8, & \tau_1 \in D_{j+2} \cup D_{j+5}. \end{cases}$$

Case 2. $\tau_2 = 1, 0 \leq \tau_1 < p$. In this case, one has

$$L^\tau(v) = I(L^{\tau_1+d+\eta}(s_j) + b(1), L^{\tau_1+2d}(s_i) + b(2), L^{\tau_1+3d+\eta}(s'_j) + b(3), L^{\tau_1+1}(s_i) + b(0)).$$

Then the autocorrelation of v at shift $\tau = 4\tau_1 + 1$ is equal to

$$\begin{aligned}
 R_v(\tau) &= (-1)^{b(0)+b(1)} \left(R_{s_i, s_j}(\tau_1 + d + \eta) - R_{s_i, s'_j}(\tau_1 + d + \eta) \right) \\
 &\quad + (-1)^{b(1)+b(2)} \left(R_{s_j, s_i}(\tau_1 + d - \eta) - R_{s'_j, s_i}(\tau_1 + d - \eta) \right) \\
 &= 2(-1)^{b(0)+b(1)} (-1)^{s_i(-(\tau_1+d+\eta))} + 2(-1)^{b(1)+b(2)} (-1)^{s_i(\tau_1+d-\eta)} \\
 &= \pm 2 \left((-1)^{s_i(-(\tau_1+d+\eta))} \pm (-1)^{s_i(\tau_1+d-\eta)} \right).
 \end{aligned}$$

Obviously, $R_v(\tau) \in \{0, \pm 4\}$.

Case 3. $\tau_2 = 2$, $0 \leq \tau_1 < p$. In this case, one has

$$L^\tau(v) = I(L^{\tau_1+2d}(s_i) + b(2), L^{\tau_1+3d+\eta}(s'_j) + b(3), L^{\tau_1+1}(s_i) + b(0), L^{\tau_1+d+\eta+1}(s_j) + b(1)).$$

Then the autocorrelation of v at shift $\tau = 4\tau_1 + 2$ is

$$\begin{aligned}
 R_v(\tau) &= 2(-1)^{b(0)+b(2)} R_{s_i}(\tau_1 + 2d) + (-1)^{b(1)+b(3)} \left(R_{s_j, s'_j}(\tau_1 + 2d) + R_{s'_j, s_j}(\tau_1 + 2d) \right) \\
 &= (-1)^{b(0)+b(2)} \left(2R_{s_i}(\tau_1 + 2d) - R_{s_j, s'_j}(\tau_1 + 2d) - R_{s'_j, s_j}(\tau_1 + 2d) \right) \\
 &= (-1)^{b(0)+b(2)} \left(2R_{s_i}(\tau_1 + 2d) - R_{s_j}(\tau_1 + 2d) + 2(-1)^{s_j(-(\tau_1+2d))} \right. \\
 &\quad \left. - R_{s_j}(\tau_1 + 2d) + 2(-1)^{s_j(\tau_1+2d)} \right) \\
 &= 2(-1)^{b(0)+b(2)} \left((-1)^{s_j(-(\tau_1+2d))} + (-1)^{s_j(\tau_1+2d)} \right) \\
 &= 2(-1)^{b(0)+b(2)} A_j(\tau_1 + 2d),
 \end{aligned}$$

where $A_j(\tau_1 + 2d)$ is defined by (3.4). From (3.5) and $A_j(\tau_1 + 2d) = 2$ if $\tau_1 + 2d \equiv 0 \pmod{p}$, we get

$$R_v(\tau) = \begin{cases} -4(-1)^{b(0)+b(2)}, & (\tau_1 + 2d) \pmod{p} \in D_j \cup D_{j+3}, \\ 0, & (\tau_1 + 2d) \pmod{p} \in D_{j+1} \cup D_{j+4}, \\ 4(-1)^{b(0)+b(2)}, & (\tau_1 + 2d) \pmod{p} \in D_{j+2} \cup D_{j+5} \cup \{0\}. \end{cases}$$

Case 4. $\tau_2 = 3$, $0 \leq \tau_1 < p$. In this case, one has

$$L^\tau(v) = I(L^{\tau_1+3d+\eta}(s'_j) + b(3), L^{\tau_1+1}(s_i) + b(0), L^{\tau_1+d+\eta+1}(s_j) + b(1), L^{\tau_1+2d+1}(s_i) + b(2)).$$

Then the autocorrelation of v at shift $\tau = 4\tau_1 + 3$ is equal to

$$\begin{aligned}
 R_v(\tau) &= (-1)^{b(0)+b(3)} \left(R_{s_i, s'_j}(\tau_1 + 3d + \eta) - R_{s_i, s_j}(\tau_1 + 3d + \eta) \right) \\
 &\quad + (-1)^{b(0)+b(1)} \left(R_{s_j, s_i}(\tau_1 + 3d - \eta) - R_{s'_j, s_i}(\tau_1 + 3d - \eta) \right) \\
 &= -2(-1)^{b(0)+b(3)} (-1)^{s_i(-(\tau_1+3d+\eta))} + 2(-1)^{b(0)+b(1)} (-1)^{s_i(\tau_1+3d-\eta)}.
 \end{aligned}$$

Since the values of $-2(-1)^{b(0)+b(3)} (-1)^{s_i(-(\tau_1+3d+\eta))} + 2(-1)^{b(0)+b(1)} (-1)^{s_i(\tau_1+3d-\eta)} \in \{0, \pm 4\}$, it follows that $R_v(\tau) \in \{0, \pm 4\}$.

Summarizing the results in all cases, we have $R_v(\tau) \in \{0, \pm 4, -8\}$. The proof of this theorem is complete.

4 Linear Complexity

In this section, we determine both the linear complexity and minimal polynomial of the two classes of binary sequences u and v defined in (3.1) and (3.3) by studying their sequence polynomials. Note that the sequence polynomial of a periodic sequence s is computed modulo $x^p - 1$, where p is the period of s .

Let m be the order of 2 modulo p . Then the splitting field of $x^p - 1$ is the finite field \mathbb{F}_{2^m} of characteristic 2. In the rest of this paper, we will denote one of the primitive p th root of unity of $x^p - 1$ in \mathbb{F}_{2^m} by β . Then β^i with $0 \leq i < p$ are exactly all roots of $x^p - 1$. The following facts about the roots of some polynomials will be needed in the sequel, we give them without proof.

Lemma 4.1 Let β be a primitive p th root of unity of $x^p - 1$ in \mathbb{F}_{2^m} . Then

- (i) β^i with $0 \leq i < p$ are exactly all roots of $x^{2p} - 1$, each with multiplicity 2;
- (ii) β^i with $0 \leq i < p$ are exactly all roots of $x^{4p} - 1$, each with multiplicity 4;
- (iii) β^i with $1 \leq i < p$ are exactly all roots of $\frac{x^{4p}-1}{x^4-1}$, each with multiplicity 4, and $\frac{x^{4p}-1}{x^4-1}|_{x=1} = 1 \neq 0$.

Lemma 4.2 Let $b = (b(0), b(1), b(2), b(3))$ be a perfect sequence and $P_b(x) = b(0) + b(1)x + b(2)x^2 + b(3)x^3$ be the sequence polynomial of b . Then $P_b(1) = 1$, i.e., $(x-1) \nmid P_b(x)$.

4.1 Linear Complexity of the First Class of Sequences u

Theorem 4.3 The linear complexity of the first class of binary sequences u defined by (3.1) is given by

$$LC(u) = \begin{cases} 3p + 1, & \eta = 0, \\ 4p, & 0 < \eta < p. \end{cases}$$

Proof By Lemmas 2.5 and 2.6(i), the sequence polynomial of u is

$$\begin{aligned} P_u(x) &= P_{s_i}(x^4) + x^{3p-4\eta}P_{s_j}(x^4) + x^{2p}P_{s_i}(x^4) \\ &\quad + x^{2p} + x^{p-4\eta}P_{s_j}(x^4) + x^{p-4\eta} + P_b(x)\frac{x^{4p}-1}{x^4-1} \\ &= (1 + x^{2p})P_{s_i}(x^4) + x^{p-4\eta}(1 + x^{2p})P_{s_j}(x^4) \\ &\quad + x^{2p} + x^{p-4\eta} + P_b(x)\frac{x^{4p}-1}{x^4-1}. \end{aligned}$$

We now distinguish two cases.

If $0 < \eta < p$, then by Lemmas 4.1(i)(iii) and 4.2, we have $P_u(1) = 1$ and $P_u(\beta^i) = 1 + \beta^{4i(p-\eta)} \neq 0$ for all i with $1 \leq i < p$. It follows from Lemma 4.1(ii) that $\gcd(P_u(x), x^{4p} - 1) = 1$, so that the minimal polynomial of u is $m_u(x) = x^{4p} - 1$ and the linear complexity of u is $LC(u) = 4p$ by Lemma 2.4.

If $\eta = 0$, then we have $P_u(x) = (1 + x^{2p})P_{s_i}(x^4) + x^p(1 + x^{2p})P_{s_j}(x^4) + x^{2p} + x^p + P_b(x)\frac{x^{4p}-1}{x^4-1}$. Also by Lemmas 4.1 and 4.2, we get $P_u(1) = 1$ and $P_u(\beta^i) = 0$ for all i with $1 \leq i < p$. So

$$\begin{aligned} \gcd(P_u(x), x^{4p} - 1) &= \gcd(P_u(x), \frac{x^{4p} - 1}{x^4 - 1}) \\ &= \gcd((1 + x^{2p})P_{s_i}(x^4) + x^p(1 + x^{2p})P_{s_j}(x^4) + x^{2p} + x^p, \frac{x^{4p} - 1}{x^4 - 1}) \\ &= \frac{x^p - 1}{x - 1} \cdot \gcd((x - 1)l(x), (\frac{x^p - 1}{x - 1})^3), \end{aligned}$$

where $l(x) = (1 + x^p)P_{s_i}(x^4) + x^p(1 + x^p)P_{s_j}(x^4) + x^p$. Since $l(\beta^i) = 1$ for $1 \leq i < p$ and β^i with $1 \leq i < p$ are exactly all distinct roots of $(\frac{x^p-1}{x-1})^3$, each with multiplicity 3, it follows that $\gcd((x - 1)l(x), (\frac{x^p-1}{x-1})^3) = 1$. Then we get $\gcd(P_u(x), x^{4p} - 1) = \frac{x^p-1}{x-1}$, and so the minimal polynomial of u is $m_u(x) = (x - 1)(x^p - 1)^3$ and the linear complexity of u is $LC(u) = 3p + 1$ by Lemma 2.4.

The proof is complete.

4.2 Linear Complexity of the Second Class of Sequences v

Theorem 4.4 The linear complexity of the second class of binary sequences v defined by (3.3) is given by

$$LC(v) = \begin{cases} 4p - 1, & b \in \{(0, 0, 1, 0), (1, 0, 0, 0), (0, 1, 1, 1), (1, 1, 0, 1)\}, \\ 4p - 2, & b \in \{(0, 1, 0, 0), (1, 0, 1, 1)\}, \\ 4p - 3, & b = (0, 0, 0, 1), \\ 4p - 4, & b = (1, 1, 1, 0). \end{cases}$$

Proof By Lemmas 2.5 and 2.6(i), the sequence polynomial of v is

$$\begin{aligned} P_v(x) &= P_{s_i}(x^4) + x^{3p-4\eta}P_{s_j}(x^4) + x^{2p}P_{s_i}(x^4) \\ &\quad + x^{p-4\eta}P_{s_j}(x^4) + x^{p-4\eta} + P_b(x)\frac{x^{4p} - 1}{x^4 - 1} \\ &= (1 + x^{2p})P_{s_i}(x^4) + x^{p-4\eta}(1 + x^{2p})P_{s_j}(x^4) \\ &\quad + x^{p-4\eta} + P_b(x)\frac{x^{4p} - 1}{x^4 - 1}. \end{aligned} \tag{4.1}$$

By Lemmas 4.1 and 4.2, we have $P_v(1) = 0$ and $P_v(\beta^i) = \beta^{4i(p-\eta)} \neq 0$ for any $1 \leq i < p$. So

$$\gcd(P_v(x), x^{4p} - 1) = \gcd(P_v(x), (x - 1)^4) = (x - 1)^k \tag{4.2}$$

for some integer k with $1 \leq k \leq 4$ by Lemma 4.1(ii). Next, we will determine the value of k . Define

$$h_1(x) = x^{p-4\eta} + P_b(x)\frac{x^{4p} - 1}{x^4 - 1}. \tag{4.3}$$

Then

$$\begin{aligned}
 h_1(x) &= P_b(x)(x^{4(p-1)} + x^{4(p-2)} + \cdots + x^{p+1} + x^{p-3} + x^{p-7} + \cdots + x^4 + 1) + x^{p-4\eta} \\
 &= P_b(x)(x^{4(p-1)} + x^{4(p-2)} + \cdots + x^{p+1} + x^{p-3} + x^{p-3} + x^{p-7} + \cdots + x^4 + 1) \\
 &\quad + x^{p-4\eta} - P_b(x)x^{p-3} \\
 &= P_b(x)(x^{4(p-2)}(1+x^4) + \cdots + x^{p-3}(1+x^4) + x^{p-7}(1+x^4) + \cdots + (1+x^4)) \\
 &\quad + x^{p-4\eta} - P_b(x)x^{p-3} \\
 &= P_b(x)(1+x^4)(x^{4(p-2)} + \cdots + x^{p-3} + x^{p-7} + \cdots + 1) + x^{p-4\eta} - P_b(x)x^{p-3} \quad (4.4)
 \end{aligned}$$

Note that $x^{p-4\eta} \equiv x^p \pmod{x^4 - 1}$. This together with (4.1), (4.2), (4.3), (4.4) and Lemma 2.6(ii) implies that

$$\gcd(P_v(x), x^{4p} - 1) = \gcd((1+x^p)(1+x^{2p}) + x^p - P_b(x)x^{p-3}, (x-1)^4). \quad (4.5)$$

Define

$$h_2(x) = (1+x^p)(1+x^{2p}) + x^p - P_b(x)x^{p-3}. \quad (4.6)$$

Next, we divide the discussion into four cases.

Case 1. $b \in \{(0, 0, 1, 0), (1, 0, 0, 0), (0, 1, 1, 1), (1, 1, 0, 1)\}$. If $b = (0, 0, 1, 0)$, then we have

$$\begin{aligned}
 h_2(x) &= (1+x^p)(1+x^{2p}) + x^p - x^{p-1} \\
 &= (1+x^p)(1+x^{2p}) + x^{p-1}(1+x).
 \end{aligned}$$

Since $(1+x) \parallel x^{p-1}(1+x)$ and $(1+x)^3 \parallel (1+x^p)(1+x^{2p})$, where $f(x)^i \parallel g(x)$ denotes that $f(x)^i \mid g(x)$ but $f(x)^{i+1} \nmid g(x)$, it follows that $\gcd(h_2(x), (x-1)^4) = x-1$. Together with (4.5) and (4.6), we have $\gcd(P_v(x), x^{4p} - 1) = x-1$, i.e., $k = 1$ in (4.2). Therefore, the minimal polynomial of v is $m_v(x) = \frac{x^{4p}-1}{x-1}$ and the linear complexity of v is $LC(v) = 4p-1$ by Lemma 2.4. For $b \in \{(1, 0, 0, 0), (0, 1, 1, 1), (1, 1, 0, 1)\}$, the result can be shown in the same way.

Case 2. $b \in \{(0, 1, 0, 0), (1, 0, 1, 1)\}$. For $b = (0, 1, 0, 0)$, we have

$$\begin{aligned}
 h_2(x) &= (1+x^p)(1+x^{2p}) + x^p - x^{p-2} \\
 &= (1+x^p)(1+x^{2p}) + x^{p-2}(1+x^2).
 \end{aligned}$$

Since $(1+x)^2 \parallel x^{p-2}(1+x^2)$ and $(1+x)^3 \parallel (1+x^p)(1+x^{2p})$, $\gcd(h_2(x), (x-1)^4) = (x-1)^2$. Together with (4.5) and (4.6), we have $\gcd(P_v(x), x^{4p} - 1) = (x-1)^2$, i.e., $k = 2$ in (4.2). Therefore, the minimal polynomial of v is $m_v(x) = \frac{x^{4p}-1}{(x-1)^2}$ and the linear complexity of v is $LC(v) = 4p-2$ by Lemma 2.4. For $b = (1, 0, 1, 1)$, the result can be obtained similarly.

Case 3. $b = (0, 0, 0, 1)$. Then $h_2(x) = (1+x^p)(1+x^{2p})$. Since $(1+x)^3 \parallel (1+x^p)(1+x^{2p})$, $\gcd(h_2(x), (x-1)^4) = (x-1)^3$. Together with (4.5) and (4.6), we have $\gcd(P_v(x), x^{4p} - 1) = (x-1)^3$, i.e., $k = 3$ in (4.2). Therefore, the minimal polynomial of v is $m_v(x) = \frac{x^{4p}-1}{(x-1)^3}$ and the linear complexity of v is $LC(v) = 4p-3$ by Lemma 2.4.

Case 4. $b = (1, 1, 1, 0)$. Then

$$\begin{aligned} h_2(x) &= (1+x^p)(1+x^{2p})+x^p-(1+x+x^2)x^{p-3} \\ &= (1+x^p)(1+x^{2p})+x^{p-3}(1+x+x^2+x^3) \\ &= (1+x)^3(1+x+x^2+\cdots+x^{p-1})^3+x^{p-3}(1+x)^3 \\ &= (1+x)^3\left((1+x+x^2+\cdots+x^{p-1})^3+x^{p-3}\right). \end{aligned}$$

Since $(1+x)|(1+x+x^2+\cdots+x^{p-1})^3+x^{p-3}$, $\gcd(h_2(x), (x-1)^4) = (x-1)^4$. Together with (4.5) and (4.6), we have $\gcd(P_v(x), x^{4p}-1) = (x-1)^4$, i.e., $k = 4$ in (4.2). Therefore, the minimal polynomial of v is $m_v(x) = \frac{x^{4p}-1}{(x-1)^4}$ and the linear complexity of v is $LC(v) = 4p-4$ by Lemma 2.4. Thus the proof of Theorem 4.4 is in all cases complete.

Example 1 Let $p = 31 = 4 + 27$. To ensure $3 \in D_1$, we use a primitive root $g = 3$ of $p = 31$ to define the cyclotomic classes of order 6. Then

$$D_0 = \{1, 2, 4, 8, 16\}, \quad D_1 = \{3, 6, 12, 17, 24\}, \quad D_2 = \{5, 9, 10, 18, 20\},$$

$$D_3 = \{15, 23, 27, 29, 30\}, \quad D_4 = \{7, 14, 19, 25, 28\}, \quad D_5 = \{11, 13, 21, 22, 26\}.$$

The six Hall's sextic residue sequences s_i of period 31 with support sets $C_i = D_i \cup D_{i+1} \cup D_{i+3}$, $i = 0, 1, \dots, 5$ are, respectively,

$$s_0 = (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1),$$

$$s_1 = (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0),$$

$$s_2 = (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1),$$

$$s_3 = (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1),$$

$$s_4 = (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0),$$

$$s_5 = (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0).$$

Take $b = (0, 0, 0, 1)$, $i = 0$, $j = 1$, $\eta = 1$, and $d = 8$. By (3.1), the interleaved sequence u of period $4p = 124$ is

$$\begin{aligned} u &= I(s_0, L^9(s_1), L^{16}(s'_0), L^{25}(s'_1) + 1) \\ &= (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, \\ &\quad 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, \\ &\quad 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, \\ &\quad 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0). \end{aligned}$$

By Magma program, the out-of-phase autocorrelation of u is

$$\begin{aligned} (R_u(\tau))_{\tau=1}^{123} = & (4, 8, 0, -4, -4, -4, -4, -4, 4, -4, -4, 0, 0, -4, 0, -4, 8, -4, -4, -8, \\ & -4, -4, -4, 0, 4, -4, 0, 0, 4, 8, -4, -4, -4, -4, -4, -8, -4, -4, 4, -8, \\ & -4, -4, -4, -8, 0, 8, 0, 0, 8, -4, 4, -8, 4, 8, 4, 0, 4, 8, -8, -4, 4, 0, 4, \\ & -4, -8, 8, 4, 0, 4, 8, 4, -8, 4, -4, 8, 0, 0, 8, 0, -8, -4, -4, -4, -8, 4, \\ & -4, -4, -8, -4, -4, -4, -4, -4, 8, 4, 0, 0, -4, 4, 0, -4, -4, -4, -8, \\ & -4, -4, 8, -4, 0, -4, 0, 0, -4, -4, 4, -4, -4, -4, -4, -4, 0, 8, 4), \end{aligned}$$

and the linear complexity of u is $LC(u) = 124$, which are coincident with the results given by Theorem 3.1 and Theorem 4.3.

Take $b = (0, 0, 1, 0)$, $i = 2$, $j = 5$, $\eta = 5$, and $d = 8$. By (3.3), the interleaved sequence v of period $4p = 124$ is

$$\begin{aligned} v = & I(s_2, L^{13}(s_5), L^{16}(s_2) + 1, L^{29}(s'_5)) \\ = & (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, \\ & 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, \\ & 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, \\ & 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0). \end{aligned}$$

By Magma program, the out-of-phase autocorrelation of v is

$$\begin{aligned} (R_v(\tau))_{\tau=1}^{123} = & (-4, 0, 0, -4, 0, -4, -4, -4, 4, 4, -4, -8, -4, -4, 0, -4, 0, 4, 0, 0, -4, \\ & 4, 0, -8, 4, 4, 4, -8, 0, 0, 0, -4, 0, -4, -4, 0, -4, -4, 0, 0, 4, 4, 0, 0, \\ & 0, 0, 0, -8, 4, -4, 4, 0, -4, 0, 4, -8, 0, 0, 0, -4, 4, -4, 4, -4, 0, 0, 0, \\ & -8, 4, 0, -4, 0, 4, -4, 4, -8, 0, 0, 0, 0, 0, 4, 4, 0, 0, -4, -4, 0, -4, -4, \\ & 0, -4, 0, 0, 0, -8, 4, 4, 4, -8, 0, 4, -4, 0, 0, 4, 0, -4, 0, -4, -4, -8, \\ & -4, 4, 4, -4, -4, -4, 0, -4, 0, 0, -4), \end{aligned}$$

and the linear complexity of v is $LC(v) = 123$, which are coincident with the results given by Theorem 3.2 and Theorem 4.4.

5 Conclusion

Theoretically, the next smallest values which are the closest to optimal autocorrelation magnitude for the out-of-phase autocorrelation values of binary sequence s of period $N \equiv 0 \pmod{4}$ are $\{0, \pm 4, 8\}$, $\{0, \pm 4, -8\}$ or $\{0, \pm 4, \pm 8\}$. In this paper, we propose two classes of binary interleaved sequences of period $4p$ by interleaving four suitable base sequences chosen from Hall's sextic residue sequences and their modified versions. The results show that the out-of-phase autocorrelation values of our proposed sequences are the closest to

the optimal autocorrelation magnitude. Moreover the proposed sequences are also shown to have very large linear complexity. Especially, when $\eta \neq 0$, the linear complexity of the first class of sequences is equal to the period of the sequences. Noting the multiple choices of base sequences and the parameter η , our construction can generate a great number of binary sequences with low autocorrelation sidelobes and large linear complexity.

References

- [1] Cusick T W, Ding C S, Renvall A. Stream ciphers and number theory[M]. Amsterdam, The Netherlands: North-Holland/Elsevier, 1998.
- [2] Ding C S, Xiao G Z, Shan W J. The stability theory of stream ciphers[M]. Berlin, Germany: Springer-Verlag, 1991.
- [3] Fan P Z, Darnell M. Sequence design for communications applications[M]. New York: Wiley, 1996.
- [4] Golomb S W, Gong G. Signal design for good correlation: for wireless communication, cryptography, and radar[M]. Cambridge, U.K.: Cambridge University Press, 2005.
- [5] Jungnickel D, Pott A. Perfect and almost perfect sequences[J]. Discret. Appl. Math., 1999, 95: 331–359.
- [6] Tang X H, Gong G. New constructions of binary sequences with optimal autocorrelation value/magnitude[J]. IEEE Trans. Inf. Theory, 2010, 56(3): 1278–1286.
- [7] Jungnickel D, Pott A. Difference sets: an introduction[A]. Pott A, Kumar P V, Hellesteth T, Jungnickel D. Difference sets, sequences and their correlation properties[C], Netherlands: Springer, 1999: 259–295.
- [8] Yu N Y, Gong G. New binary sequences with optimal autocorrelation magnitude[J]. IEEE Trans. Inf. Theory, 2008, 54(10): 4471–4479.
- [9] Massey J. Shift-register synthesis and BCH decoding[J]. IEEE Trans. Inf. Theory, 1969, 15(1): 122–127.
- [10] Gong G. Theory and applications of q -ary interleaved sequences[J]. IEEE Trans. Inf. Theory, 1995, 41(2): 400–411.
- [11] Arasu K T, Ding C S, Hellesteth T, Kumar P V, Martinsen H M. Almost difference sets and their sequences with optimal autocorrelation[J]. IEEE Trans. Inf. Theory, 2001, 47(7): 2934–2943.
- [12] Tang X H, Ding C S. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value[J]. IEEE Trans. Inf. Theory, 2010, 56(12): 6398–6405.
- [13] Xiong H, Qu L J, Li C, Fu S J. Linear complexity of binary sequences with interleaved structure[J]. IET Commun., 2013, 7: 1688–1696.
- [14] Li N, Tang X H. On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude[J]. IEEE Trans. Inf. Theory, 2011, 57(11): 7597–7604.
- [15] Su W, Yang Y, Fan C L. New optimal binary sequences with period $4p$ via interleaving Ding-Hellesteth-Lam sequences[J]. Des. Codes Cryptogr., 2018, 86(6): 1329–1338.
- [16] Ding C S, Hellesteth T, Lam K Y. Several classes of sequences with three-level autocorrelation[J]. IEEE Trans. Inf. Theory, 1999, 45(7): 2606–2612.
- [17] Fan C L. The linear complexity of a class of binary sequences with optimal autocorrelation[J]. Des. Codes Cryptogr., 2018, 86(10): 2441–2450.
- [18] Ding C S. Linear complexity of generalized cyclotomic binary sequences of order 2[J]. Finite Fields Appl., 1997, 3: 159–174.

- [19] Ding C S, Helleseht T, Shan W J. On the linear complexity of Legendre sequences[J]. IEEE Trans. Inf. Theory, 1998, 44(3): 1276–1278.
- [20] Storer T. Cyclotomy and Difference Sets[M]. Chicago: Markham Publishing Co., 1967.
- [21] Hall M. A survey of difference sets[J]. Proc. Amer. Math. Soc., 1956, 7: 975–986.
- [22] Lidl R, Niederreiter H. Finite fields[M]. Cambridge: Cambridge University Press, 1997.
- [23] Wang Q, Du X N. The linear complexity of binary sequences with optimal autocorrelation[J]. IEEE Trans. Inf. Theory, 2010, 56(12): 6388–6397.

两类具有低自相关和大线性复杂度的 $4p$ 周期二元序列

杨 波, 朱自坤, 肖自碧

(武汉科技大学理学院, 湖北 武汉 430065)

摘要: 具有良好自相关性质和大线性复杂度的二元序列设计对于通信系统和流密码的各种应用非常重要. 本文从Hall六次剩余序列和它们的修改版本中选取4条合适的序列作为基序列, 利用交织技术构造了两类周期为 $4p$ 的二元序列, 并且完全确定了这两类序列的自相关和线性复杂度. 研究结果表明这两类序列既具有低自相关性质又具有非常大的线性复杂度.

关键词: 二元序列; 交织结构; 自相关; 线性复杂度

MR(2010)主题分类号: 11T22; 11T55; 94A55; 94A60

中图分类号: O157.4