New Binary Sequences with Optimal Autocorrelation Magnitude

Nam Yul Yu, *Student Member, IEEE* and Guang Gong, *Member, IEEE*

Department of Electrical and Computer Engineering

University of Waterloo, Canada

Abstract

New binary sequences of period $N = 4(2^m - 1)$ for even $m \geq 4$ are found. These sequences can be described by a $4 \times (2^m - 1)$ interleaved structure. The new sequences are almost balanced and have four-valued autocorrelation, i.e., $\{N, 0, \pm 4\}$, which is optimal with respect to autocorrelation magnitude. Complete autocorrelation distribution and exact linear complexity of the sequences are mathematically derived. From the simple implementation with a small number of shift registers and a connector, the sequences have a benefit of obtaining large linear complexity.

Index Terms

Binary sequences, interleaved sequences, linear complexity, optimal autocorrelation.

I. INTRODUCTION

Binary pseudorandom sequences with optimal autocorrelation play important roles in many areas of communication and cryptography. In code-division multiple access (CDMA) communication systems, the sequences are needed to acquire accurate timing information of received signals. In cryptography, on the other hand, the sequences are used to generate key streams in stream cipher encryptions.

For binary sequences of period $N = 2^m - 1$, binary m-sequences are traditionally well-known sequences with ideal two-level autocorrelation of $\{N, -1\}$. Due to their good randomness properties and simple implementation [9] [10], m-sequences have been widely used for communication systems. Besides m-sequences, several other inequivalent classes of binary sequences with ideal two-level autocorrelation have been constructed and discovered [4] [13] [20] [22] [24].

For binary sequences of even period N, on the other hand, Lempel, Cohn, and Eastman [16] showed that $1)$ autocorrelation must have at least two distinct out-of-phase values and $2)$ a difference between any two autocorrelation values is divisible by 4. Therefore, optimal autocorrelation is $\{N, 2, -2\}$ if $N \equiv 2 \pmod 4$, and $\{N, 0, -4\}$ or $\{N, 0, 4\}$ if $N \equiv 0 \pmod 4$. Several classes of binary sequences of even period with optimal autocorrelation are known. Initially, Lempel, Cohn, and Eastman [16] presented a class of the balanced binary sequences of period $N = p^m - 1$ for odd prime p. (It is known that this has been already described in [25] and called as the *Sidelnikov sequences*.) Then, No, Chung, Song, Yang, Lee, and Helleseth [23] gave another class of the binary sequences of period $N = p^m - 1$ for odd prime p using a polynomial $(z + 1)^d + az^d + b$ over a finite field. From a group division structure by the Chinese Remainder theorem, Ding, Helleseth, and Martinsen [6] also presented several families of the binary sequences of period $N = 2p$ for odd prime $p \equiv 5 \pmod 8$ which correspond to almost difference sets. Using known cyclic difference sets, Arasu, Ding, Helleseth, Kumar, and Martinsen [1] constructed four classes of almost difference sets which give inequivalent classes of the binary sequences of period $N \equiv 0 \pmod 4$. These sequences generally contain the binary sequences of period $N \equiv 0 \pmod 4$ constructed from the product method in [18]. Recently, Zhang, Lei, and Zhang [27] presented an almost difference set corresponding to the binary sequence of period $N \equiv 0 \pmod 4$ by adding two indices to one class of the almost difference set in [1] where the corresponding cyclic difference set is from the Legendre sequences.

For a period $N \equiv 0 \pmod 4$, the autocorrelation $\{N, 0, -4\}$ or $\{N, 0, 4\}$ is optimal from the Lempel, Cohn, and Eastman's assertion in the sense that it has the two out-of-phase values with the smallest magnitudes. If we allow three out-of-phase values with the smallest magnitudes, on the other hand, then optimal autocorrelation should be $\{N, 0, \pm 4\}$, where the autocorrelation is *optimal with respect to its magnitude*. In practical applications, we believe that it has the same meaning as conventional optimal autocorrelation. Consequently, the autocorrelation of $\{N, 0, \pm 4\}$ is also considered as optimal in this correspondence.

In [11], Gong introduced the interleaved structure of sequences which is indeed a good method not only for understanding a sequence structure, but also for constructing new sequences of an interleaved form [11] [12]. In this correspondence, we show that a binary sequence of period $4(2^m - 1)$ shown in [1] can be represented by a $(2^m - 1) \times 4$ interleaved structure. We also show that a binary product sequence [18] of period $4(2^m - 1)$ with optimal autocorrelation can be represented as a $4 \times (2^m - 1)$ interleaved structure. Inspired by these interpretations, we discover a new construction of binary sequences of period $N = 4(2^m - 1)$ with autocorrelation $\{N, 0, \pm 4\}$ by the interleaved method. In details, we use a $4 \times (2^m - 1)$ interleaved structure defined by a perfect binary sequence of period 4 and a binary m-sequence of period $2^m - 1$. In the interleaved structure, a sequence defined over $\mathbb{Z}_4$ is used as a shift sequence. The new sequences are almost balanced, i.e., a difference between the numbers of zeros and ones in a period is 2 [23], and optimal with respect to autocorrelation magnitude. Complete autocorrelation distribution and exact linear complexity of the sequences are mathematically derived. From the simple implementation with a small number of shift registers and a connector, the sequences have a benefit of obtaining large linear complexity.

This correspondence is organized as follows. In Section II, we give preliminary concepts and definitions on binary sequences for understanding this correspondence. Interleaved structures of known binary sequences of period $4(2^m - 1)$ with optimal autocorrelation are presented in Section III. In Section IV, new binary sequences of period $N = 4(2^m - 1)$ for even $m \geq 4$ with autocorrelation $\{N, 0, \pm 4\}$ are constructed using a $4 \times (2^m - 1)$ interleaved structure, and the autocorrelation distribution is mathematically derived. In Section V, linear complexity of the sequences is investigated and the implementation is discussed. Concluding remarks are given in Section VI.

II. Preliminaries

Following notation will be used throughout this correspondence.

- $\mathbb{Z}_m$ is a ring of integers modulo m, and $\mathbb{Z}_m^+ = \{r \in \mathbb{Z}_m | r \neq 0\}$.
- $\mathbb{F}_q = GF(q)$ is a finite field with q elements and $\mathbb{F}_q^*$ is a multiplicative group of $\mathbb{F}_q$.
- For a binary sequence $\mathbf{a} = \{a_t\}$, $a_t \in \{0, 1\}$. $\overline{\mathbf{a}}$ is a complement of $\mathbf{a}$, or $\overline{\mathbf{a}} = \{a_t + 1\}$ where the addition is computed modulo 2.
- For a sequence $\mathbf{a} = \{a_t\}$ over $\mathbb{F}_q$ and an integer g, $\mathbf{a} + g = \{a_t + g\}$ where the addition is computed modulo q.
- For positive integers n and m, let $m|n$. A trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is denoted by $Tr_m^n(x)$, i.e.,

$$Tr_m^n(x) = x + x^{2^m} + \cdots + x^{2^{m(\frac{n}{m}-1)}}, \quad x \in \mathbb{F}_{2^n},$$

  or simply as $Tr(x)$ if $m = 1$ and the context is clear.

A. *Equivalence of Sequences*

Let $\mathbf{a} = \{a_t\}$ and $\mathbf{b} = \{b_t\}$ be two periodic sequences. Then, they are called *cyclically equivalent* [10] if there exists an integer k such that

$$a_t = b_{t+k} \text{ for all } t \geq 0.$$

Otherwise, they are called *cyclically distinct*.

B. *Balance and Almost Balance Properties*

Let $\mathbf{a} = \{a_t\}$ be a binary sequence of period N. Then $\mathbf{a}$ is called *balanced* [9] if the number of zeros is nearly equal to the number of ones in a period, i.e.,

$$S = \left| \sum_{t=0}^{N-1} (-1)^{a_t} \right| \leq 1$$

where S denotes a difference between the numbers of zeros and ones of a binary sequence in a period. For odd N, $\mathbf{a}$ is balanced if and only if $S = 1$, and for even N, it is balanced if and only if $S = 0$. On the other hand, if N is even and $S = 2$, then $\mathbf{a}$ is called *almost balanced* [23].

C. *Autocorrelation*

(Periodic) autocorrelation of a binary sequence $\mathbf{a} = \{a_t\}$ of period N is defined by

$$C_{\mathbf{a}}(\tau) = \sum_{t=0}^{N-1} (-1)^{a_{t+\tau}+a_t}, \quad 0 \leq \tau \leq N-1$$

where τ is a phase shift of $\mathbf{a}$ and the indices are computed modulo N. For a sequence $\mathbf{a}$ of period N, it is implied that $C_{\mathbf{a}}(\tau) = N$ occurs only at $\tau \equiv 0 \pmod{N}$. $C_{\mathbf{a}}(\tau)$ is called *optimal autocorrelation* [1] if it satisfies

1) $C_{\mathbf{a}}(\tau) \in \{N, -1\}$ if $N \equiv 3 \pmod 4$, or
2) $C_{\mathbf{a}}(\tau) \in \{N, 1, -3\}$ if $N \equiv 1 \pmod 4$, or
3) $C_{\mathbf{a}}(\tau) \in \{N, 2, -2\}$ if $N \equiv 2 \pmod 4$, or
4) $C_{\mathbf{a}}(\tau) \in \{N, 0, -4\}$ or $\{N, 0, 4\}$ if $N \equiv 0 \pmod 4$

for all τ. In particular, case 1) is called *ideal two-level autocorrelation* and a binary sequence of case 1) corresponds to a *cyclic difference set* [2] [14]. Complete classes of all the known inequivalent binary sequences of period $N = 2^m - 1$ with ideal two-level autocorrelation and the corresponding cyclic difference sets are summarized in [4].

Binary sequences of cases 2) - 4) are described by *almost difference sets* [6] and the other methods. Several classes of binary sequences of cases 2) and 3) are described by the corresponding almost difference sets in [5] and [6], respectively. On the other hand, four classes of binary sequences of case 4) and the corresponding almost difference sets are presented in [1] where the sequences generally contain the binary sequences constructed from the product method in [18]. Another almost difference set corresponding to a binary sequence of case 4) is presented in [27] by adding two indices to one class of the almost difference sets in [1]. From a finite field approach, furthermore, binary sequences of period $N = p^m - 1$ for odd prime p corresponding to cases 3) and 4) are also described in [16] and [23], respectively. For a survey of binary and quadriphase sequences with optimal autocorrelation, see [19].

In this correspondence, if $C_{\mathbf{a}}(\tau) \in \{N, 0, \pm 4\}$ for $N \equiv 0 \pmod 4$, we consider that it is also optimal in the sense that *its autocorrelation magnitude is identical to that of case 4).*

D. Perfect Sequences

Let $\mathbf{a}$ be a binary sequence of period N. If autocorrelation $C_{\mathbf{a}}(\tau)$ is equal to 0 for all $\tau \not\equiv 0 \pmod N$, then $\mathbf{a}$ is called a *perfect sequence*. A perfect sequence is also defined for a nonbinary sequence by extending the definition of its autocorrelation [10]. For nonbinary cases, a few polyphase perfect sequences are known in [7] and [8]. However, the only known perfect binary sequence is $\mathbf{a} = (0, 1, 1, 1)$ or its complement [2]. For a period of $4 < N < 108900$, no perfect binary sequences are discovered [26], and it is conjectured in [15] that no other perfect binary sequences exist except for $N = 4$.

E. Product Sequences

Let $\mathbf{a}$ and $\mathbf{b}$ be binary sequences of periods N_1 and N_2, respectively, where $\gcd(N_1, N_2) = 1$. Then a *product sequence* [18] $\mathbf{p} = \mathbf{a} + \mathbf{b} = (p_0, p_1, \cdots, p_{N-1})$ of period $N = N_1 N_2$ is defined by a component-wise addition of $p_t = a_t + b_t,\ 0 \le t \le N - 1$ where the addition is computed modulo 2. Autocorrelation of the product sequence is given by

$$\begin{aligned} C_{\mathbf{p}}(\tau) &= \sum_{t=0}^{N-1} (-1)^{p_{t+\tau}+p_t} = \left[\sum_{t_1=0}^{N_1-1} (-1)^{a_{t_1+\tau}+a_{t_1}}\right] \cdot \left[\sum_{t_2=0}^{N_2-1} (-1)^{b_{t_2+\tau}+b_{t_2}}\right] \\ &= C_{\mathbf{a}}(\tau) \cdot C_{\mathbf{b}}(\tau), \quad 0 \le \tau \le N-1 \end{aligned} \tag{1}$$

where the indices of a sequence are computed modulo its own period [18].

F. Almost Difference Set (ADS) Sequences of Period $N \equiv 0 \pmod 4$

In [1], Arasu, Ding, Helleseth, Kumar, and Martinsen presented binary sequences of period $N \equiv 0 \pmod 4$ with optimal autocorrelation. Let $\mathbf{a} = \{a_t\}$ be a binary sequence of period v with ideal two-level autocorrelation and a matrix $G = (g_{x,y}), 0 \le x \le 3, 0 \le y \le v-1$ be defined by

$$G = \begin{bmatrix} a_0 & a_1 & \cdots & a_{v-1} \\ \overline{a}_\eta & \overline{a}_{\eta+1} & \cdots & \overline{a}_{v-1+\eta} \\ \overline{a}_0 & \overline{a}_1 & \cdots & \overline{a}_{v-1} \\ \overline{a}_\eta & \overline{a}_{\eta+1} & \cdots & \overline{a}_{v-1+\eta} \end{bmatrix} \tag{2}$$

where η is any integer in $0 \le \eta \le v-1$ and the indices are computed modulo v. A binary sequence $\mathbf{s} = \{s_t\}$ of period $N = 4v$ is defined by

$$s_t = g_{x,y} \quad \text{where } x \equiv t \pmod 4 \text{ and } y \equiv t \pmod v. \tag{3}$$

Then $\mathbf{s}$ has optimal autocorrelation of $C_{\mathbf{s}}(\tau) \in \{N, 0, -4\}$ for every $\eta, 0 \le \eta \le v-1$ by providing the corresponding almost difference set [1]. Throughout this correspondence, $\mathbf{s}$ is called an *ADS sequence*.

G. Interleaved Sequences

Let $\mathbf{u} = \{u_t\}$ be a binary sequence of period vw where both v and w are not equal to 1. Then, we can arrange $\mathbf{u}$ by an $v \times w$ matrix, i.e.,

$$U = (\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{w-1}) = \begin{bmatrix} u_0 & u_1 & \cdots & u_{w-1} \\ u_w & u_{w+1} & \cdots & u_{2w-1} \\ \vdots & \vdots & \cdots & \vdots \\ u_{(v-1)w} & u_{(v-1)w+1} & \cdots & u_{vw-1} \end{bmatrix}.$$

If each column $\mathbf{u}_j$ is either a cyclic shift of a binary sequence $\mathbf{a}$ of period v or a zero sequence, then $\mathbf{u}$ is called a binary (v, w) *interleaved sequence* [11]. According to the definition, $\mathbf{u}_j = L^{e_j}(\mathbf{a}),\ 0 \le j \le w-1$ where L^{e_j} denotes a cyclic e_j left shift operation, and $e_j \in \mathbb{Z}_v$ or $e_j = \infty$ if $\mathbf{u}_j = (0, 0, \cdots, 0)$. Here, a transpose notation is omitted because we consider it as a sequence. In the interleaved sequence, $\mathbf{a} = (a_0, a_1, \cdots, a_{v-1})$ and $\mathbf{e} = (e_0, e_1, \cdots, e_{w-1})$ are called a *base sequence* and a *shift sequence* of $\mathbf{u}$, respectively. In this correspondence, the matrix U is used for an array form of $\mathbf{u}$, denoted by $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) = U$.

In $\mathbf{w} = \mathbf{u} + \mathbf{b} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$, the (v, w) interleaved structure is preserved by adding a binary sequence $\mathbf{b}$ of period w. Let $W = (\mathbf{w}_0, \cdots, \mathbf{w}_{w-1}) = \mathbf{w}$. In W, $\mathbf{b} = \{b_j | 0 \leq j \leq w-1\}$ is used as an *indicator sequence* where $\mathbf{w}_j = \mathbf{u}_j$ if $b_j = 0$, or $\mathbf{w}_j = \overline{\mathbf{u}}_j$ otherwise.

H. Interleaved Structure of Binary m-sequences

Let $m = 2k$ and $\mathbf{u}$ be a binary m-sequence of period $2^m - 1$ represented by $u_t = Tr_1^m(\alpha^t),\ 0 \leq t \leq 2^m - 2$ where α is a primitive element of $\mathbb{F}_{2^m}$. (As a binary m-sequence, we consider a sequence satisfying the *constant-on-cosets* property [10].) Then, $\mathbf{u}$ is represented by a $(2^k - 1, 2^k + 1)$ interleaved sequence [11], i.e., $\mathbf{u} = A(\mathbf{a}, \mathbf{e})$. In its array form $U = (\mathbf{u}_0, \cdots, \mathbf{u}_{2^k})$, a base sequence $\mathbf{a}$ is a binary m-sequence of period $2^k - 1$ represented by $a_i = Tr_1^k(\beta^i),\ 0 \leq i \leq 2^k - 2$ where $\beta = \alpha^{2^k+1}$ is a primitive element of $\mathbb{F}_{2^k}$. Also, a shift sequence $\mathbf{e}$ is given by

$$e_j = \begin{cases} \infty, & j = 0 \\ Tr_k^m(\alpha^j), & 1 \leq j \leq 2^k. \end{cases}$$

In other words, $\mathbf{u}_0$ is a zero sequence of length $2^k - 1$, and $\mathbf{u}_j,\ j \neq 0$ is a cyclic e_j shift of a binary m-sequence $\mathbf{a}$ of period $2^k - 1$.

III. Interleaved Structures of Known Binary Sequences with Optimal Autocorrelation

In this section, we examine interleaved structures of binary sequences of period $N = 4(2^m - 1)$ with optimal autocorrelation. First, a $(2^m - 1) \times 4$ interleaved structure of the ADS sequence is given using a binary sequence of period $2^m - 1$ with ideal two-level autocorrelation and the constant-on-cosets property as a base sequence. Then, a product sequence with optimal autocorrelation is also examined by a $4 \times (2^m - 1)$ interleaved structure where each column is a cyclic shift of a perfect binary sequence of period 4.

A. ADS Sequences

In the ADS sequence $\mathbf{s}$ defined by (3), let $v = 2^m - 1$ and $\mathbf{a}$ be a binary sequence of period $2^m - 1$ with ideal two-level autocorrelation and the constant-on-cosets property. If we represent

$\mathbf{s}$ by a $(2^m-1)\times 4$ interleaved structure, then

$$\mathbf{s}=\begin{bmatrix} a_0 & \overline{a}_{1+\eta} & \overline{a}_2 & \overline{a}_{3+\eta} \\ a_4 & \overline{a}_{5+\eta} & \overline{a}_6 & \overline{a}_{7+\eta} \\ \vdots & \vdots & \vdots & \vdots \\ a_{4(2^m-1)-4} & \overline{a}_{4(2^m-1)-3+\eta} & \overline{a}_{4(2^m-1)-2} & \overline{a}_{4(2^m-1)-1+\eta} \end{bmatrix}=(\mathbf{s}_0,\mathbf{s}_1,\mathbf{s}_2,\mathbf{s}_3)$$

where $\mathbf{s}_j=\{s_{i,j}\}, 0\le i\le 2^m-2, 0\le j\le 3$ and η is an integer, $0\le\eta\le 2^m-2$. From the constant-on-cosets property of $\mathbf{a}$ and $4^{-1}\equiv 2^{m-2} \pmod{2^m-1}$, we have

1) $s_{i,0}=a_{4i}=a_i$,
2) $s_{i,1}=\overline{a}_{4i+1+\eta}=\overline{a}_{4(i+4^{-1}(1+\eta))}=\overline{a}_{4(i+2^{m-2}(1+\eta))}=\overline{a}_{i+2^{m-2}(1+\eta)}$,
3) $s_{i,2}=\overline{a}_{4i+2}=\overline{a}_{4(i+4^{-1}\cdot 2)}=\overline{a}_{4(i+2^{m-1})}=\overline{a}_{i+2^{m-1}}$,
4) $s_{i,3}=\overline{a}_{4i+3+\eta}=\overline{a}_{4(i+4^{-1}(3+\eta))}=\overline{a}_{4(i+2^{m-2}(3+\eta))}=\overline{a}_{i+2^{m-2}(3+\eta)}$

where the indices are computed modulo 2^m-1. From this, we have the following interleaved structure of $\mathbf{s}$.

Property 1: Let $\mathbf{s}$ be the ADS sequence of period $4(2^m-1)$. Then, $\mathbf{s}$ has a $(2^m-1)\times 4$ interleaved structure, i.e., $\mathbf{s}=A(\mathbf{a},\mathbf{e})+\mathbf{b}$ where

1) $\mathbf{a}$ is a binary sequence of period 2^m-1 with ideal two-level autocorrelation and the constant-on-cosets property,
2) $\mathbf{e}=(e_0,e_1,e_2,e_3)=(0,2^{m-2}(\eta+1),2^{m-1},2^{m-2}(\eta+3))$ is a shift sequence,
3) $\mathbf{b}=(0,1,1,1)$ is a perfect binary sequence

where η is an integer, $0\le\eta\le 2^m-2$.

From the interleaved structure, $\mathbf{s}$ is cyclically distinct for each $\eta, 0\le\eta\le 2^m-2$. If $\eta=0$, in particular, it is pointed out in [1] that $\mathbf{s}$ is equivalent to a product sequence of $\mathbf{a}$ and $\mathbf{b}$, i.e., $\mathbf{s}=\mathbf{a}+\mathbf{b}$. Thus, a product sequence of period $4(2^m-1)$ with optimal autocorrelation is a special case of the ADS sequence.

Example 1: For $m=3$, let $\mathbf{a}$ be a binary m-sequence of period 7, i.e., $\mathbf{a}=(1,0,0,1,0,1,1)$.

If $\eta = 1$, then $\mathbf{e} = (0, 4, 4, 1)$. Then, the corresponding ADS sequence $\mathbf{s}$ is given by

$$\mathbf{s} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = (1,1,1,1,0,0,0,1,0,0,0,0,1,0,0,1,0,1,1,0,1,1,1,0,1,0,0,0).$$

B. Product Sequences

In Section III-A, a product sequence of period $4(2^m - 1)$ with optimal autocorrelation is represented by a $(2^m - 1) \times 4$ interleaved structure as a special case of the ADS sequence ($\eta = 0$). Here, we show that it is also represented by a $4 \times (2^m - 1)$ interleaved structure with different base and shift sequences.

Let $\mathbf{p} = \mathbf{a} + \mathbf{b}$ be a binary product sequence of period $4(2^m - 1)$ where $\mathbf{a} = (0, 1, 1, 1)$ is a perfect binary sequence of period 4 and $\mathbf{b}$ a binary sequence of period $2^m - 1$ with ideal two-level autocorrelation. Then $\mathbf{p}$ has optimal autocorrelation from (1). Note that $\gcd(4, 2^m - 1) = 1$ and $2^m - 1 \equiv 3 \pmod 4$ for any integer $m > 1$. We first consider a $4 \times (2^m - 1)$ interleaved structure $M = (\mathbf{m}_0, \mathbf{m}_1, \cdots, \mathbf{m}_{2^m-2})$ associated with $\mathbf{a}$ of length $4(2^m - 1)$. Then, $\mathbf{m}_j$ is given by

$$\mathbf{m}_j = \{a_{(2^m-1)i+j}\}, \quad 0 \le i \le 3,\ 0 \le j \le 2^m - 2$$

where the index is computed modulo 4. From $3^{-1} \equiv 3 \pmod 4$ and $a_{3i} = a_i$, we have

$$a_{(2^m-1)i+j} = a_{3i+j} = a_{3(i+3^{-1}j)} = a_{3(i+3j)} = a_{i+3j}. \tag{4}$$

Thus, the product sequence $\mathbf{p}$ has the following interleaved structure.

Property 2: Let $\mathbf{p} = \mathbf{a} + \mathbf{b}$ be a binary product sequence of period $4(2^m - 1)$ with optimal autocorrelation. Then, it has a $4 \times (2^m - 1)$ interleaved structure, i.e., $\mathbf{p} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$ where

1) $\mathbf{a} = (0, 1, 1, 1)$ is a perfect binary sequence,
2) $\mathbf{e} = (e_0, e_1, \cdots, e_{2^m-2})$ is a shift sequence defined over $\mathbb{Z}_4$ where the j-th element is given by

$$e_j \equiv 3j \pmod 4, \quad 0 \le j \le 2^m - 2, \tag{5}$$

3) $\mathbf{b}$ is a binary sequence of period $2^m - 1$ with ideal two-level autocorrelation.

In the interleaved structure of $\mathbf{p} = (\mathbf{p}_0, \cdots, \mathbf{p}_{2^m-2})$, its j-th column is given by $\mathbf{p}_j = L^{e_j}(\mathbf{a})$ if $b_j = 0$, or $\mathbf{p}_j = L^{e_j}(\overline{\mathbf{a}})$ otherwise.

Example 2: For $m = 4$, a product sequence of period $N = 4 \times 15 = 60$ with optimal autocorrelation is given by $\mathbf{p} = \mathbf{a} + \mathbf{b}$ where $\mathbf{a} = (0, 1, 1, 1)$, a perfect binary sequence of period 4, and $\mathbf{b} = (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$, a binary m-sequence of period 15. From (5), $\mathbf{e}$ is defined by

$$\mathbf{e} = (0, 3, 2, 1, 0, 3, 2, 1, 0, 3, 2, 1, 0, 3, 2).$$

Then, $\mathbf{p}$ is given by

$$\mathbf{p} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Now, we focus on a shift sequence over $\mathbb{Z}_4$ of the product sequence of period $N = 4(2^m - 1), m = 2k$ for an integer $k > 1$ with optimal autocorrelation. For $m = 2k$, the shift sequence shown in (5) can also be represented by a $(2^k - 1) \times (2^k + 1)$ interleaved structure, i.e.,

$$\begin{aligned} \mathbf{e} = (e_0, e_1, \cdots, e_{2^m-2}) &= \begin{bmatrix} e_0 & e_1 & \cdots & e_{2^k} \\ e_{2^k+1} & e_{2^k+2} & \cdots & e_{2\cdot 2^k+1} \\ \vdots & \vdots & \cdots & \vdots \\ e_{(2^k-2)(2^k+1)} & e_{(2^k-2)(2^k+1)+1} & \cdots & e_{2^m-2} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 3 & 2 & 1 & 0 & 3 & 2 & 1 & \cdots & 0 \\ 3 & 2 & 1 & 0 & 3 & 2 & 1 & 0 & \cdots & 3 \\ 2 & 1 & 0 & 3 & 2 & 1 & 0 & 3 & \cdots & 2 \\ \vdots & & & & \vdots & & & & \cdots & \vdots \\ 2 & 1 & 0 & 3 & 2 & 1 & 0 & 3 & \cdots & 2 \end{bmatrix}. \end{aligned}$$

Interestingly, the $(2^k - 1) \times (2^k + 1)$ interleaved structure of $\mathbf{e}$ is given by

$$\begin{aligned} &\mathbf{e} = (\mathbf{e}_0, \mathbf{e}_1, \cdots, \mathbf{e}_{2^k}) \\ &\text{where } \mathbf{e}_j = \{e_{i,j}\}, \;\; e_{i,j} = 3(i + j) \pmod 4, \;\; 0 \le i \le 2^k - 2, \;\; 0 \le j \le 2^k. \end{aligned} \tag{6}$$

Note that $e_{i,j} = e_{i(2^k+1)+j}$ and both expressions are used throughout this correspondence.

In next section, we will give a new construction of binary sequences of period $N = 4(2^m - 1)$ for even $m \geq 4$ with optimal four-valued autocorrelation by modifying the shift sequence of the interleaved structure of a product sequence.

IV. New Binary Sequences with Optimal Four-valued Autocorrelation

In this section, we present a new construction of binary sequences of period $N = 4(2^m - 1)$ for even $m \geq 4$ with optimal four-valued autocorrelation, i.e., $C_{\mathbf{u}}(\tau) \in \{N, 0, \pm 4\}$ for any τ.

A. Construction

Construction 1: Let $k > 1$ be a positive integer. A new binary sequence $\mathbf{u}$ of period $N = 4(2^m - 1), m = 2k$ is defined by a $4 \times (2^m - 1)$ interleaved structure of $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$ where

1) $\mathbf{a} = (0, 1, 1, 1)$ is a perfect binary sequence of period 4,

2) $\mathbf{b}$ is a binary m-sequence of period $2^m - 1$ with the constant-on-cosets property,

3) $\mathbf{e}$ is a sequence defined over $\mathbb{Z}_4$ of period $2^m - 1$, and represented by a $(2^k - 1) \times (2^k + 1)$ interleaved structure, i.e.,

$$\mathbf{e} = (\mathbf{e}_0, \mathbf{e}_1, \cdots, \mathbf{e}_{2^k})$$

$$\text{where } \mathbf{e}_j = \{e_{i,j}\},\ e_{i,j} = \begin{cases} 3i + \delta \pmod 4, & \text{if } j = 0 \\ 3(i+j) \pmod 4, & \text{if } 1 \leq j \leq 2^k \end{cases} \qquad (7)$$

where $0 \leq i \leq 2^k - 2$ and $\delta = 1$ or -1.

In fact, the new sequence $\mathbf{u}$ is obtained by modifying the shift sequence of (6) in the interleaved structure of a product sequence.

Remark 1: With $\delta = \pm 1$ and cyclically distinct binary m-sequences of $\mathbf{b}$, Construction 1 gives $\frac{2\phi(2^m-1)}{m}$ cyclically distinct binary sequences $\mathbf{u}$, where $\phi(\cdot)$ is the Euler-totient function.

Theorem 1: Let $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$ be the binary sequence from Construction 1. Then $\mathbf{u}$ is almost balanced.

Proof: In the $4 \times (2^m - 1)$ interleaved structure of $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$, note that the l-th column is a cyclic shift of either $\mathbf{a} = (0, 1, 1, 1)$ or $\overline{\mathbf{a}}$, which is determined by $\mathbf{b} = \{b_l\}$. In other words, each column of $\mathbf{u}$ has 3 ones if $b_l = 0$, or 1 ones if $b_l = 1$. Since $\mathbf{b}$ is a binary m-sequence of period $2^m - 1$ with the balance property [10], the number of ones in $\mathbf{u}$ is given by

$$3(2^{m-1} - 1) + 2^{m-1} = 2^{m+1} - 3 = \frac{N}{2} - 1.$$

Hence, a difference between the numbers of zeros and ones in a period is 2, i.e., $\mathbf{u}$ is almost balanced. ■

B. Autocorrelation

To compute the autocorrelation function of $\mathbf{u}$, we first consider Proposition 1.

Proposition 1: Let $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$ be the binary sequence from Construction 1. Let $\tau = r(2^m - 1) + s,\ 0 \le r \le 3,\ 0 \le s \le 2^m - 2$. Then the autocorrelation function $C_{\mathbf{u}}(\tau)$ is given by

$$C_{\mathbf{u}}(\tau) = \sum_{t=0}^{N-1} (-1)^{u_t + u_{t+\tau}} = \sum_{l=0}^{2^m-2} (-1)^{d_l} C_{\mathbf{a}}(t_l) \tag{8}$$

where $d_l \equiv b_l - b_{l+s} \pmod 2$, $t_l \equiv e_{l+s} - e_l + r \pmod 4$, and $C_{\mathbf{a}}(t_l)$ is autocorrelation of a base sequence $\mathbf{a}$. In b_{l+s}, the index is computed modulo $2^m - 1$. As in equation (12) of [12], on the other hand,

$$e_{l+s} \equiv e_{l+s-(2^m-1)} + 1 \pmod 4 \text{ if } l + s \ge 2^m - 1. \tag{9}$$

Proof: From $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$, it is immediate from Lemma 2 of [12]. ■

In Construction 1, note that the indicator sequence $\mathbf{b}$ and the shift sequence $\mathbf{e}$ have the $(2^k - 1) \times (2^k + 1)$ interleaved structures. Then, $\mathbf{d} = \{d_l | 0 \le l \le 2^m - 2\}$ in Proposition 1 is represented by a difference array $D = B - B_s$ where $(2^k - 1) \times (2^k + 1)$ arrays B and B_s represent $\mathbf{b} = \{b_l\}$ and $L^s(\mathbf{b}) = \{b_{l+s}\}$, respectively. From the shift-and-add property [10] of the binary m-sequence $\mathbf{b}$, it is clear that $D = (\mathbf{d}_0, \cdots, \mathbf{d}_{2^k})$ also represents a binary m-sequence of period $2^m - 1$. Also, the j-th column $\mathbf{d}_j, 0 \le j \le 2^k$ is either a cyclic shift of a binary m-sequence of period $2^k - 1$ or a zero sequence from the interleaved structure of binary m-sequences. In the following lemma, we further study a structure of the array D. From now on, we use following notation in all lemmas and theorems in Section IV.

$$\begin{gathered} \tau = r(2^m - 1) + s, \quad 0 \le r \le 3,\ 0 \le s \le 2^m - 2 \\ \text{where } s = x(2^k + 1) + y, \quad 0 \le x \le 2^k - 2,\ 0 \le y \le 2^k \end{gathered} \tag{10}$$

Lemma 1: Let B and B_s be $(2^k-1)\times(2^k+1)$ arrays of $\mathbf{b}$ and $L^s(\mathbf{b})$, respectively, where $s\neq 0$. In the difference array $D=B-B_s=(\mathbf{d}_0,\cdots,\mathbf{d}_{2^k})$, the j-th column $\mathbf{d}_j$ has the following properties.

1) If $y=0$, then a zero column $\mathbf{d}_j$ exists only at $j=0$.
2) If $y\neq 0$, then a zero column $\mathbf{d}_j$ exists at exactly one j for $0\leq j\leq 2^k$ with $j\neq 0$ and $j\neq -y$ where '$-y$' is computed modulo 2^k+1.

Proof: In $B=(\mathbf{b}_0,\cdots,\mathbf{b}_{2^k})$, $\mathbf{b}_0$ is a zero column and $\mathbf{b}_j, j\neq 0$ is a cyclic shift of a binary m-sequence from Section II-H. In another array $B_s=(\mathbf{s}_0,\cdots,\mathbf{s}_{2^k})$ of $L^s(\mathbf{b})$, on the other hand, $\mathbf{s}_{-y}$ is a zero column and $\mathbf{s}_j, j\neq -y$ is a cyclic shift of a binary m-sequence. In the difference $D=B-B_s$, therefore, $\mathbf{d}_0$ is still a zero column if $y=0$. If $y\neq 0$, on the other hand, neither $\mathbf{d}_0=\mathbf{b}_0-\mathbf{s}_0$ nor $\mathbf{d}_{-y}=\mathbf{b}_{-y}-\mathbf{s}_{-y}$ can be a zero column because both $\mathbf{s}_0$ and $\mathbf{b}_{-y}$ are nonzero columns. Instead, a zero column $\mathbf{d}_j$ exists at another column index j with $j\neq 0$ and $j\neq -y$ because there should be exactly one zero column in the difference array D which represents a binary m-sequence. This completes a proof of Lemma 1. ■

In Proposition 1, $\mathbf{t}=\{t_l|0\leq l\leq 2^m-2\}$ can also be represented by a $(2^k-1)\times(2^k+1)$ interleaved structure T. To obtain T, we need the following two lemmas.

Lemma 2: In the array structure of $\mathbf{e}$ in (7), s-shift $L^s(\mathbf{e})$ of $\mathbf{e}$ is given by

$$L^s(\mathbf{e})=(\mathbf{e}_y-x,\mathbf{e}_{1+y}-x,\cdots,\mathbf{e}_{2^k+y}-x) \tag{11}$$

where $\mathbf{e}_j$ is defined in Construction 1 and extended to $\mathbf{e}_j=\mathbf{e}_{j-(2^k+1)}+3 \pmod 4$ for $j\geq 2^k+1$.

Proof: If we arrange $L^s(\mathbf{e})$ in an array form, then we have

$$L^s(\mathbf{e})=\begin{bmatrix} e_{x,y} & \cdots & e_{x,2^k} & e_{x+1,0} & \cdots & e_{x+1,y-1} \\ e_{x+1,y} & \cdots & e_{x+1,2^k} & e_{x+2,0} & \cdots & e_{x+2,y-1} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ e_{2^k-3,y} & \cdots & e_{2^k-3,2^k} & e_{2^k-2,0} & \cdots & e_{2^k-2,y-1} \\ e_{2^k-2,y} & \cdots & e_{2^k-2,2^k} & e_{0,0}+1 & \cdots & e_{0,y-1}+1 \\ e_{0,y}+1 & \cdots & e_{0,2^k}+1 & e_{1,0}+1 & \cdots & e_{1,y-1}+1 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ e_{x-1,y}+1 & \cdots & e_{x-1,2^k}+1 & e_{x,0}+1 & \cdots & e_{x,y-1}+1 \end{bmatrix} \tag{12}$$

where the '$+1$' addition is from (9) and computed modulo 4. From the definition of $e_{i,j}$ in (7),

$$e_{i+1,j} - e_{i,j} \equiv 3 \pmod 4, \quad 0 \le i \le 2^k - 3. \tag{13}$$

Also,

$$e_{0,j} + 1 - e_{2^k-2,j} = 3j + 1 + \Delta - 3(2^k - 2 + j) - \Delta \equiv 3 \pmod 4, \quad 0 \le j \le 2^k \tag{14}$$

where $\Delta = \delta = \pm 1$ if $j = 0$, or $\Delta = 0$ otherwise. From (13) and (14), we see that in (12), every element in a difference vector between the $(i+1)$-th row and the i-th row for $0 \le i \le 2^k - 3$ is 3 $(\mathrm{mod}\ 4)$. Thus, we can write (12) as

$$L^s(\mathbf{e}) = (\mathbf{e}_y + 3x, \cdots, \mathbf{e}_{2^k} + 3x, \mathbf{e}_0 + 3x + 3, \cdots, \mathbf{e}_{y-1} + 3x + 3)$$

For $j \ge 2^k + 1$, if $\mathbf{e}_j$ is defined by $\mathbf{e}_j = \mathbf{e}_{j-(2^k+1)} + 3 \pmod 4$, then $L^s(\mathbf{e})$ is given by (11) from $3x \equiv -x \pmod 4$. ■

Lemma 3: With the notation of Proposition 1 and Lemma 2, let $l = i(2^k + 1) + j$ where $0 \le l \le 2^m - 2$, $0 \le i \le 2^k - 2$, and $0 \le j \le 2^k$. Then, $t_l \equiv e_{l+s} - e_l + r \pmod 4$ is given by

$$t_l = \begin{cases} 3y - x + r, & \text{if } j \ne 0 \text{ and } j + y \not\equiv 0 \pmod{2^k + 1}, \\ 3y - x + r + \delta, & \text{if } j \ne 0 \text{ and } j + y \equiv 0 \pmod{2^k + 1}, \\ 3y - x + r - \delta, & \text{if } j = 0 \text{ and } j + y \not\equiv 0 \pmod{2^k + 1}, \\ -x + r, & \text{if } j = 0 \text{ and } j + y \equiv 0 \pmod{2^k + 1}. \end{cases} \tag{15}$$

In a $(2^k - 1) \times (2^k + 1)$ array $T = (\mathbf{t}_0, \cdots, \mathbf{t}_{2^k})$ of $\mathbf{t} = \{t_l\}$, each column has constant elements given as follows.

1) If $y = 0$, then

$$\mathbf{t}_j = \{t_{i,j} = -x + r | 0 \le i \le 2^k - 2\} \text{ for all } 0 \le j \le 2^k. \tag{16}$$

2) If $y \ne 0$, then

$$\begin{aligned} \mathbf{t}_0 &= \{t_{i,0} = 3y - x + r - \delta | 0 \le i \le 2^k - 2\}, \\ \mathbf{t}_{-y} &= \{t_{i,-y} = 3y - x + r + \delta | 0 \le i \le 2^k - 2\}, \\ \mathbf{t}_j &= \{t_{i,j} = 3y - x + r | 0 \le i \le 2^k - 2\} \text{ for } j \ne 0 \text{ and } j + y \not\equiv 0 \pmod{2^k + 1} \end{aligned} \tag{17}$$

where '$-y$' is computed modulo $2^k + 1$.

Proof: A $(2^k-1)\times(2^k+1)$ array structure of $\mathbf{t}$ is given by

$$T = L^s(\mathbf{e}) - \mathbf{e} + r$$

where r is added to all elements of the array. From Lemma 2, we see that the j-th column vector of T is given by

$$\mathbf{t}_j = \mathbf{e}_{j+y} - \mathbf{e}_j - x + r = \{e_{i,j+y} - e_{i,j} - x + r | 0 \le i \le 2^k - 2\}, \quad 0 \le j \le 2^k.$$

From $l = i(2^k+1)+j$, it is clear that t_l is the i-th element of $\mathbf{t}_j$, i.e.,

$$t_l = e_{l+s} - e_l + r = e_{i,j+y} - e_{i,j} - x + r. \tag{18}$$

Together with (18) and (7), (15) follows immediately. The assertions of (16) and (17) are from (15). ■

Now, we are ready to compute $C_{\mathbf{u}}(\tau)$.

Theorem 2: Let $\mathbf{u} = A(\mathbf{a},\mathbf{e}) + \mathbf{b}$ be the binary sequence of period $N = 4(2^m-1), m = 2k$ for an integer $k > 1$ from Construction 1. Then it has four-valued optimal autocorrelation, i.e., $C_{\mathbf{u}}(\tau) \in \{N, 0, \pm 4\}$ for any τ. Precisely, its complete autocorrelation is given by

$$C_{\mathbf{u}}(\tau) = \begin{cases} 4(2^m-1), & \text{if } \tau = 0 \\ 0, & \text{if } (\tau \neq 0 \text{ and } s = 0) \text{ or } (s,y,v) = (\sigma,0,\nu) \text{ or } (y,v) = (\psi,2) \\ -4, & \text{if } (s,y,v) = (\sigma,0,0) \text{ or } (y,v) = (\psi,1) \text{ or } (y,v) = (\psi,3) \\ +4, & \text{if } (y,v) = (\psi,0) \end{cases}$$

where $s \equiv \tau \pmod{2^m-1}$, $y \equiv \tau \pmod{2^k+1}$, and $v \equiv \tau \pmod 4$ for some $\sigma \in \mathbb{Z}^+_{2^m-1}$, $\psi \in \mathbb{Z}^+_{2^k+1}$, and $\nu \in \mathbb{Z}^+_4$.

Proof: To compute $C_{\mathbf{u}}(\tau)$, we use (8) in Proposition 1. Since $C_{\mathbf{a}}(t_l) = 0$ for nonzero t_l, nonzero $C_{\mathbf{u}}(\tau)$ is determined by cases of $t_l = 0$ in (8). We have the following three cases. Recall (10) and the arrays D and T of $\mathbf{d} = \{d_l\}$ and $\mathbf{t} = \{t_l\}$ in Lemmas 1 and 3, respectively.

Case 1. $s = 0$: If $r = 0$ in this case, then $\tau = 0$ and $C_{\mathbf{u}}(\tau) = 4(2^m-1)$, a trivial in-phase autocorrelation. If $r \neq 0$, on the other hand, $t_l = e_{j+s} - e_j + r = r \neq 0$ and then $C_{\mathbf{u}}(\tau) = 0$ in (8) because $C_{\mathbf{a}}(t_l) = 0$ for all nonzero t_l. Thus, we have

$$C_{\mathbf{u}}(\tau) = \begin{cases} 4(2^m-1), & \text{if } \tau = 0, \\ 0, & \text{if } \tau \neq 0 \text{ and } s = 0. \end{cases} \tag{19}$$

Case 2. $s \neq 0$ and $y = 0$: From (16), T is a constant array where each element is $-x + r$ and D is balanced from the difference property of m-sequences, i.e., $\sum_{l=0}^{2^m-2}(-1)^{d_l} = -1$. If $r = x$, then $t_l = 0$ for all $0 \leq l \leq 2^m - 2$. Hence, $C_{\mathbf{u}}(\tau) = -1 \cdot C_{\mathbf{a}}(0) = -4$ from (8). If $r \neq x$, on the other hand, $t_l \neq 0$ and $C_{\mathbf{a}}(t_l) = 0$ for all $0 \leq l \leq 2^m - 2$ and hence $C_{\mathbf{u}}(\tau) = 0$. From (10), note that if $y = 0$, then $v \equiv \tau \mod 4 \equiv -r + x$. Therefore,

$$C_{\mathbf{u}}(\tau) = \begin{cases} -4, & \text{if } (s, y, v) = (\sigma, 0, 0) \\ 0, & \text{if } (s, y, v) = (\sigma, 0, \nu). \end{cases} \tag{20}$$

where σ and ν are some elements in $\mathbb{Z}_{2^m-1}^{+}$ and $\mathbb{Z}_4^{+}$, respectively.

Case 3. $s \neq 0$ and $y \neq 0$: Let $l = i(2^k + 1) + j$. From Lemma 3, we have three distinct t_l's in T, i.e., $t_l = h, h \pm 1$ where $h = 3y - x + r$. (Note that $\delta = \pm 1$ in (7).) $t_l = h$ corresponds to $\mathbf{t}_j$'s of $0 \leq j \leq 2^k$ with $j \neq 0$ and $j \neq -y$. For such j's, $\mathbf{t}_j$ is a constant column of h and there exists one j such that $\mathbf{d}_j$ is a zero column from Lemma 1. On the other hand, $t_l = h \pm 1$ corresponds to $\mathbf{t}_0$ and $\mathbf{t}_{-y}$, respectively, and both $\mathbf{d}_0$ and $\mathbf{d}_{-y}$ are nonzero m-sequences in D.

1) $h = 0$: In this case, all $\mathbf{t}_j$'s of $0 \leq j \leq 2^k$ with $j \neq 0$ and $j \neq -y$ are zero columns. On the other hand, $\mathbf{t}_0$ and $\mathbf{t}_{-y}$ are nonzero. Let n_0 and n_1 be the numbers of zeros and ones in $\mathbf{d}_j$'s for $0 \leq j \leq 2^k$ with $j \neq 0$ and $j \neq -y$. Then,

$$n_0 = (2^k - 2)(2^{k-1} - 1) + 2^k - 1 = 2^{2k-1} - 2^k + 1$$

$$n_1 = (2^k - 2)2^{k-1} = 2^{2k-1} - 2^k = n_0 - 1.$$

From (8), $C_{\mathbf{u}}(\tau) = (n_0 \cdot 1 + n_1 \cdot (-1)) \cdot C_{\mathbf{a}}(0) = 1 \cdot C_{\mathbf{a}}(0) = 4$.

2) $h = \pm 1$: In this case, either $\mathbf{t}_0$ or $\mathbf{t}_{-y}$ is a zero column for given h and δ. On the other hand, all other columns are nonzero. If n_0 and n_1 are the numbers of zeros and ones in $\mathbf{d}_0$ or $\mathbf{d}_{-y}$, then

$$n_0 = 2^{k-1} - 1, \quad n_1 = 2^{k-1} = n_0 + 1$$

Thus, $C_{\mathbf{u}}(\tau) = (n_0 \cdot 1 + n_1 \cdot (-1)) \cdot C_{\mathbf{a}}(0) = (-1) \cdot C_{\mathbf{a}}(0) = -4$.

3) $h = 2$: In this case, no columns are zero in T. Thus, $C_{\mathbf{u}}(\tau) = 0$ from $C_{\mathbf{a}}(t_l) = 0$.

From (10), note that $v \equiv \tau \mod 4 \equiv 3r + x + y \equiv 3 \cdot (3y - x + r) \equiv -h$. Combining $1)$, $2)$ and $3)$, we have

$$C_{\mathbf{u}}(\tau) = \begin{cases} +4, & \text{if } (y, v) = (\psi, 0) \\ -4, & \text{if } (y, v) = (\psi, 1) \text{ or } (y, v) = (\psi, 3) \\ 0, & \text{if } (y, v) = (\psi, 2) \end{cases} \tag{21}$$

where ψ is some element in $\mathbb{Z}_{2^k+1}^{+}$. In (21), note that $y \neq 0$ implies $s \neq 0$.

If we combine (19), (20), and (21), then the proof is completed. ■

Remark 2: In Remark 1, we have many cyclically distinct sequences of $\mathbf{u}$ according to δ and $\mathbf{b}$. In Theorem 2, however, the distinction disappears regarding their autocorrelations and consequently all the sequences from Construction 1 have identical autocorrelation distribution regardless of δ and $\mathbf{b}$.

Theorem 3: With the notation in Theorem 2, complete distribution of $C_{\mathbf{u}}(\tau)$ is given by

$$C_{\mathbf{u}}(\tau) = \begin{cases} 4(2^m-1), & 1 \text{ time} \\ 0, & 2^{2k}+2^{k+1}-3 \text{ times} \\ -4, & 2^{2k+1}-2^k-2 \text{ times} \\ +4, & 2^{2k}-2^k \text{ times.} \end{cases}$$

Proof: From Theorem 2, a trivial in-phase autocorrelation occurs only once. Hence, we count the other exclusive cases of Theorem 2.

Case 1. $C_{\mathbf{u}}(\tau) = -4$:

1) $(s, y, v) = (\sigma, 0, 0)$: In this case, possible τ's are $4(2^k+1), 8(2^k+1)\cdots, 4(2^k-2)(2^k+1)$. Thus its number of occurrences is $w_0 = 2^k - 2$.
2) $(y, v) = (\psi, 1)$ or $(\psi, 3)$: Note that $\gcd(2^k+1, 4) = 1$. By the Chinese Remainder theorem, we have a unique solution of τ for $(y, v) = (\psi, 1)$ with given $\psi \in \mathbb{Z}_{2^k+1}^{+}$. Thus, the number of distinct solutions of τ in $\mathbb{Z}_{4(2^k+1)}^{+}$ for $(y, v) = (\psi, 1)$ is 2^k for all $\psi \in \mathbb{Z}_{2^k+1}^{+}$. From the isomorphism $\mathbb{Z}_{4(2^m-1)} \cong \mathbb{Z}_{4(2^k+1)} \times \mathbb{Z}_{2^k-1}$, the number of τ's in $\mathbb{Z}_{4(2^m-1)}$ for $(y, v) = (\psi, 1)$ is $2^k(2^k-1)$. Considering the exclusive cases of $(y, v) = (\psi, 1)$ and $(\psi, 3)$, the number of such τ's is $w_1 = 2^{k+1}(2^k-1)$.

Combining $1)$ and $2)$, the number of occurrences of $C_{\mathbf{u}}(\tau) = -4$ is $\lambda_0 = w_0 + w_1 = 2^{2k+1} - 2^k - 2$.

Case 2. $C_{\mathbf{u}}(\tau) = +4$: This corresponds to $(y, v) = (\psi, 0)$. By a similar approach to Case 1-2), the number of such τ's is equal to $\lambda_1 = w_1/2 = 2^k(2^k-1)$.

Case 3. $C_{\mathbf{u}}(\tau) = 0$: The number of such τ's is $\lambda_2 = 4(2^m-1) - (1 + \lambda_0 + \lambda_1) = 2^{2k} + 2^{k+1} - 3$.

From Cases 1 - 3, the proof is completed. ■

Example 3: For $m = 2k = 4$, consider a new sequence $\mathbf{u}$ in Construction 1 with $\delta = 1$. In its interleaved structure $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$, a base sequence is $\mathbf{a} = (0, 1, 1, 1)$ and an indicator

TABLE I

AUTOCORRELATION VALUES OF $C_{\mathbf{u}}(\tau)$ IN EXAMPLE 3

τ	$C_{\mathbf{u}}(\tau)$														
$0-14$	60	-4	0	-4	4	0	0	-4	4	-4	0	-4	4	-4	0
$15-29$	0	4	-4	0	-4	-4	-4	0	-4	4	0	0	-4	4	-4
$30-44$	0	-4	4	-4	0	0	4	-4	0	-4	-4	-4	0	-4	4
$45-59$	0	0	-4	4	-4	0	-4	4	-4	0	0	4	-4	0	-4

sequence is $\mathbf{b} = (0,0,0,1,0,0,1,1,0,1,0,1,1,1,1)$, a binary m-sequence of period 15. A shift sequence $\mathbf{e}$ is defined by (7), and $\mathbf{b}$ and $\mathbf{e}$ are represented by 3×5 arrays, respectively, i.e.,

$$\mathbf{b} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad \mathbf{e} = \begin{bmatrix} 1 & 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 0 & 3 \\ 3 & 1 & 0 & 3 & 2 \end{bmatrix}.$$

Then, a new sequence $\mathbf{u}$ of period $60 = 4 \times 15$ is given by

$$\mathbf{u} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Consider $C_{\mathbf{u}}(1)$. From $\tau = 1$, we have $r = 0, s = 1, x = 0, y = 1$ from (10). D and T are given by

$$D = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad T = \begin{bmatrix} 2 & 3 & 3 & 3 & 0 \\ 2 & 3 & 3 & 3 & 0 \\ 2 & 3 & 3 & 3 & 0 \end{bmatrix}.$$

Hence, we see that Lemmas 1 and 3 are true in this case. From D and T at $\tau = 1$, we can easily compute $C_{\mathbf{u}}(1) = -4$. The autocorrelation function from Theorem 2 is shown in Table I. From Theorem 3, the complete autocorrelation distribution is given by

$$C_{\mathbf{u}}(\tau) = \begin{cases} 60, & 1 \text{ time} \\ 0, & 21 \text{ times} \\ -4, & 26 \text{ times} \\ +4, & 12 \text{ times.} \end{cases}$$

Both the autocorrelation function and the distribution are verified from computer experiments.

V. Other aspects of new binary sequences

In this section, we derive exact linear complexity of the new binary sequences and show that large linear complexity can be obtained from the sequences. Implementation of the sequences requires only a small number of shift registers and a simple logic.

Linear complexity of a sequence is defined as the shortest length of a shift register which generates the sequence, or equivalently a degree of the minimal polynomial of the sequence [10]. Before examining linear complexity of the sequence $\mathbf{u}$ from Construction 1, we consider the following lemmas.

Lemma 4: Let $\mathbf{z} = \{z_t\} = (1,1,0,0)$ or $(1,0,0,1)$. Let $\mathbf{c} = \{c_t\}$ be a binary sequence of period $n = 4(2^k+1)$ such that

$$c_t = \begin{cases} 0, & \text{if } t \neq t'(2^k+1), \\ z_{t'}, & \text{if } t = t'(2^k+1) \end{cases} \tag{22}$$

where k is a positive integer and t' is an integer, $0 \leq t' \leq 3$. Then, the minimal polynomial of $\mathbf{c}$ is $m_c(x) = (x^{2^k+1}+1)^3$.

Proof: Let $C(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1}$. From (22), $C(x)$ is given by

$$C(x) = \begin{cases} 1 + x^{2^k+1}, & \text{if } \mathbf{z} = (1,1,0,0), \\ 1 + x^{3(2^k+1)}, & \text{if } \mathbf{z} = (1,0,0,1). \end{cases}$$

From [17], the minimal polynomial of $\mathbf{c}$ is given by

$$\begin{aligned} m_c(x) &= \frac{x^n+1}{\gcd(x^n+1, C(x))} = \frac{x^{4(2^k+1)}+1}{\gcd(x^{4(2^k+1)}+1, C(x))} = \frac{(x^{2^k+1}+1)^4}{x^{2^k+1}+1} \\ &= (x^{2^k+1}+1)^3 \end{aligned}$$

for both cases of $\mathbf{z}$. ■

Lemma 5: Let $\mathbf{u} = A(\mathbf{a}, \mathbf{e}) + \mathbf{b}$ be the binary sequence from Construction 1. Then, $\mathbf{u}$ is represented by $\mathbf{u} = \mathbf{a} + \mathbf{b} + \mathbf{c}$, i.e.,

$$u_t = a_t + b_t + c_t, \quad 0 \leq t \leq 4(2^m-1)-1 \tag{23}$$

where $\mathbf{c} = \{c_t\}$ is the binary sequence from Lemma 4.

Proof: Assume that $\mathbf{u} = \mathbf{a}+\mathbf{b}+\mathbf{f}$ where $\mathbf{f} = \{f_t\}$. Since $\mathbf{u} = \mathbf{a}+\mathbf{b}$ at $t \not\equiv 0 \pmod{2^k+1}$,

$$f_t = 0 \text{ for } t \not\equiv 0 \pmod{2^k+1}. \tag{24}$$

For $t = t'(2^k + 1)$ with $0 \le t' \le 4(2^k - 1) - 1$, let $t' = i(2^k - 1) + i'$ where $0 \le i \le 3$ and $0 \le i' \le 2^k - 2$. Then,

$$t = t'(2^k + 1) = (2^m - 1)i + (2^k + 1)i' = (2^m - 1)i + j \tag{25}$$

where i and $j = (2^k + 1)i'$ correspond to row and column indices of the interleaved structure of $\mathbf{u}$, respectively. Recall the interleaved structure of a sequence $\mathbf{a}$ in (4). Then, u_t is represented as

$$u_t = a_t + b_t + f_t = a_{i+3j} + b_t + f_t \tag{26}$$

at $t = t'(2^k + 1)$. From Construction 1, on the other hand,

$$u_t = a_{i+3j+\delta} + b_t \tag{27}$$

at $t = t'(2^k + 1)$. From (25), note that $t \equiv t' \equiv 3i + j \pmod 4$. Also, $3^{-1} \equiv 3 \pmod 4$ and $a_{3i} = a_i$. Then, from (26) and (27),

$$f_t = f_{t'(2^k+1)} = a_{i+3j+\delta} + a_{i+3j} = a_{3i+j+3\delta} + a_{3i+j} = a_{t'+3\delta} + a_{t'} = h_{t'} \tag{28}$$

where $\delta = \pm 1$ and the indices are computed modulo 4. Let $\mathbf{h} = \{h_{t'}\}$. Since $\mathbf{a}$ has a period 4, $\mathbf{h}$ and $\mathbf{f}$ have periods 4 and $4(2^k + 1)$ from (28), respectively. Also, it is easily known from (28) that $\mathbf{h} = (1, 1, 0, 0)$ if $\delta = 1,$ or $\mathbf{h} = (1, 0, 0, 1)$ if $\delta = -1$ which is identical to $\mathbf{z}$ from Lemma 4. Thus,

$$f_t = z_{t'} \text{ for } t = t'(2^k + 1), \quad 0 \le t' \le 3. \tag{29}$$

From (24) and (29), $\mathbf{f} = \mathbf{c}$ in (22), and hence (23) is true. ■

Linear complexity of the binary sequences from Construction 1 is presented by Theorem 4.

Theorem 4: Let $\mathbf{u}$ be the binary sequence of period $N = 4(2^m - 1), m = 2k$ for an integer $k > 1$ from Construction 1. Then, linear complexity of $\mathbf{u}$ is given by

$$L_c = 3(1 + 2^k) + 1 + 2k.$$

Proof: By definition of the minimal polynomials, $m_u(x)$, the minimal polynomial of $\mathbf{u}$ is determined by the least common multiple (*lcm*) of the minimal polynomials of $\mathbf{a}$, $\mathbf{b}$, and $\mathbf{c}$ in Lemma 5. Let $m_a(x), m_b(x)$, and $m_c(x)$ be the minimal polynomials of $\mathbf{a}, \mathbf{b}$, and $\mathbf{c}$, respectively.

It is easily known that $m_a(x) = (x+1)^4$ and $m_b(x)$ is a primitive polynomial of degree $m = 2k$. From Lemma 4,

$$\begin{aligned} lcm(m_a(x), m_c(x)) &= lcm((x+1)^4, (x^{2^k+1}+1)^3) \\ &= lcm((x+1)^4, (x+1)^3(x^{2^k}+x^{2^k-1}+\cdots+x+1)^3) \\ &= (x+1)(x^{2^k+1}+1)^3. \end{aligned}$$

Note that $\gcd(m_b(x), x+1) = 1$ and if $k > 1$, $\gcd(m_b(x), x^{2^k+1}+1) = 1$. Finally,

$$\begin{aligned} m_u(x) &= lcm(lcm(m_a(x), m_c(x)), m_b(x)) = lcm(m_a(x), m_c(x)) \cdot m_b(x) \\ &= (x+1)(x^{2^k+1}+1)^3 \cdot m_b(x) \end{aligned}$$

where a degree of $m_u(x)$ or linear complexity of $\mathbf{u}$ is given by

$$L_c = 3(2^k+1) + 1 + m = 3(2^k+1) + 1 + 2k$$

which completes the proof. ■

Remark 3: In Theorem 4, we requested that $k > 1$. For the case of $k = 1$, the new binary sequence $\mathbf{u}$ of period 12 also has optimal autocorrelation $C_{\mathbf{u}}(\tau) \in \{12, 0, \pm 4\}$ for any τ. However, its linear complexity is $L_c = 3(2^k+1)+1 = 10$. It is because in the proof of Theorem 4, $m_b(x) = x^2+x+1$ is a factor of $m_c(x) = (x^3+1)^3$, and thus the minimal polynomial $m_u(x)$ of $\mathbf{u}$ is given by $lcm(m_a(x), m_c(x)) = (x+1)(x^3+1)^3$.

Table II shows linear complexities of the three different binary sequences of period $4(2^m-1)$ with optimal autocorrelation. For the product and the ADS sequences in Section III adopting m-sequences of period 2^m-1 as an indicator or a base sequence in their interleaved structures, their linear complexities are given by $m+4$ and $2m+4$, respectively, which will be discussed in Appendix I. In Table II, the new binary sequences from Construction 1 provides much larger linear complexity than the other two classes of sequences. Linear complexities of Table II are confirmed by computer experiments using the Berlekamp-Massey algorithm [3] [21].

Figure 1 shows implementation of the new binary sequence $\mathbf{u}$ of period $4(2^m-1)$ with $\delta = 1$. (If $\delta = -1$, we only need to change the initial state of the 3-stage LFSR from $(0,1,1)$ to $(0,0,1)$.) In Fig. 1, the 3-stage linear feedback shift register (LFSR) is enabled and connected to other LFSRs only at time $t = t'(2^k+1), t' = 0,1,2,\cdots$. In the implementation, $\mathbf{u} = \{u_t\}$ is generated by combining only $(m+7)$ shift registers and a simple connector. From Theorem 4,

TABLE II

LINEAR COMPLEXITY OF BINARY SEQUENCES OF PERIOD $4(2^{m}-1)$ WITH OPTIMAL AUTOCORRELATION ADOPTING A BINARY m-SEQUENCE

m	Period	Product Sequence	ADS Sequence	New Sequence
4	60	8	12	20
6	252	10	16	34
8	1020	12	20	60
10	4092	14	24	110
12	16380	16	28	208
14	65532	18	32	402
16	262140	20	36	788
18	1048572	22	40	1558

however, its actual linear complexity is $L_c = 3(2^k+1)+1+2k \gg 2k+7$ for $k = m/2$, where we obtain the large linear complexity with the low implementation cost.

Remark 4: Let l be linear complexity of a binary sequence of period 2^m-1 with ideal two-level autocorrelation which is used as an indicator or a base sequence of the product or the ADS sequences in Section III. Then, linear complexities of the product and the ADS sequences are $l+4$ and at most $2l+4$, respectively, which will be proved in Appendix I. If $l \gg m$, then the linear complexities can be larger than that of the new sequences from Construction 1. In this case, however, we need as many numbers of shift registers as the linear complexities for their implementation, which requires the larger implementation cost.

VI. Conclusion

From a $4 \times (2^m-1)$ interleaved structure, we have constructed new binary sequences of period $N = 4(2^m-1)$ for even $m \geq 4$ with four-valued autocorrelation $\{N, 0, \pm 4\}$ which is optimal with respect to autocorrelation magnitude. Complete autocorrelation distribution and exact linear complexity of the sequences have been mathematically derived. Only with $(m+7)$ shift registers and a simple connector, the sequences are implemented to give large linear complexity.

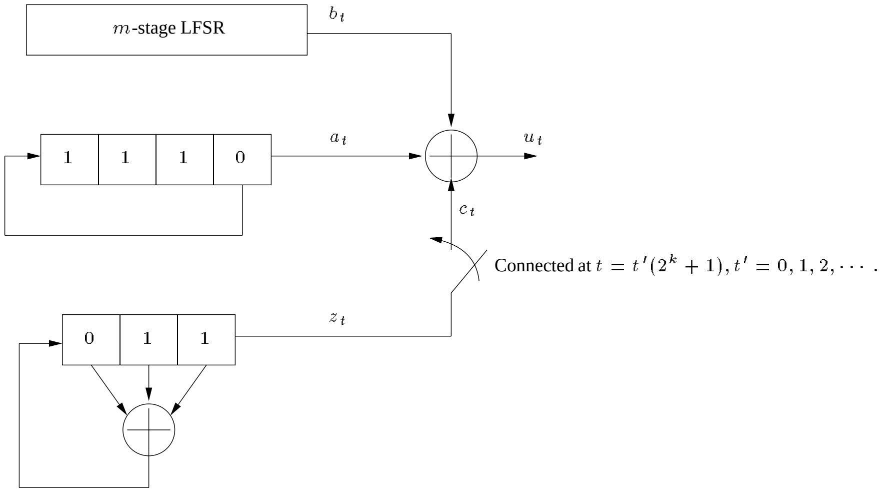

Fig. 1. Implementation of a new binary sequence of period $4(2^{\,m}-1), m=2k, k>1$ with optimal autocorrelation $(\delta = 1)$

Appendix I

In Appendix I, we show two lemmas on linear complexities of the product and the ADS sequences of period $4(2^m-1)$ in Section III.

Lemma 6: Let $\mathbf{p} = \mathbf{a}+\mathbf{b}$ be the product sequence of period $4(2^m-1)$ with optimal autocorrelation shown in Section III, where $\mathbf{a}$ is a perfect binary sequence of period 4 and $\mathbf{b}$ a binary sequence of period 2^m-1 with ideal two-level autocorrelation. Then, its linear complexity is given by $L_c = l+4$ where l is linear complexity of $\mathbf{b}$.

Proof: The minimal polynomial of a perfect binary sequence $\mathbf{a}$ is $m_a(x) = (x+1)^4$. Let $m_b(x)$ be the minimal polynomial of $\mathbf{b}$. In general, $m_b(x) = \prod_i r_i(x)$ where $r_i(x)$ is a primitive polynomial over $\mathbb{F}_2$. We assume $\gcd(m_b(x), x+1) = 1$ without loss of generality. Then the minimal polynomial of $\mathbf{p}$ is given by $m_p(x) = lcm(m_a(x), m_b(x)) = (x+1)^4 \cdot m_b(x)$. Therefore, a degree of $m_p(x)$ or linear complexity of $\mathbf{p}$ is given by $L_c = l+4$ where l is a degree of $m_b(x)$ or linear complexity of $\mathbf{b}$. ■

Lemma 7: Let $\mathbf{s}$ be the ADS sequence of period $4(2^m-1)$ defined by (3) with a binary two-level autocorrelation sequence $\mathbf{a}$ of period 2^m-1 and a matrix G in (2). If linear complexity of $\mathbf{a}$ is l, then linear complexity L_c of $\mathbf{s}$ is at most $2l+4$, i.e., $L_c \le 2l+4$. In particular, the equality is achieved if $\mathbf{a}$ is a binary m-sequence and $\eta \neq 0$.

Proof: From (2) and (3), $\mathbf{s} = \{s_t\}$ is represented by

$$\mathbf{s} = \mathbf{w} + \mathbf{b} \text{ where } s_t = w_t + b_t,\ 0 \le t \le 4(2^m - 1) - 1 \tag{30}$$

where $\mathbf{b} = \{b_t\}$ is a perfect binary sequence of period 4 and $\mathbf{w} = \{w_t\}$ is a binary sequence defined by

$$w_t = \begin{cases} a_t, & \text{if } t \equiv 0 \pmod 2 \\ a_{t+\eta}, & \text{if } t \equiv 1 \pmod 2 \end{cases} \tag{31}$$

If $\eta = 0$, we have $\mathbf{w} = \mathbf{a}$ and $\mathbf{s} = \mathbf{a} + \mathbf{b}$. Thus, the linear complexity of $\mathbf{s}$ is given by $L_c = l + 4$ from Lemma 6.

For a nontrivial ADS sequence with $\eta \neq 0$, it is clear that $\mathbf{w}$ is a binary sequence of period $2(2^m - 1)$. From (31), $\mathbf{w}$ is represented by a $(2^m - 1) \times 2$ interleaved structure where its first column is $(a_0, a_2, a_4, \cdots)$ and the second column is $(a_{1+\eta}, a_{3+\eta}, a_{5+\eta}, \cdots)$. Since each column sequence is a form of a shift-and-decimation of $\mathbf{a}$, its minimal polynomial is identical to $m_a(x)$, the minimal polynomial of $\mathbf{a}$. Let $m_w(x)$ be the minimal polynomial of $\mathbf{w}$. From the interleaved structure of $\mathbf{w}$, we have

$$m_w(x) | m_a(x^2) = (m_a(x))^2 \tag{32}$$

from Lemma 1 of [11]. Similar to the proof of Lemma 6, we assume $\gcd(m_a(x), x+1) = 1$ and thus $\gcd(m_w(x), x+1) = 1$. From (30), the minimal polynomial $m_s(x)$ of $\mathbf{s}$ is given by

$$m_s(x) = lcm(m_w(x), m_b(x)) = lcm(m_w(x), (x+1)^4) = m_w(x)(x+1)^4 \tag{33}$$

where $m_b(x) = (x+1)^4$ is the minimal polynomial of a perfect binary sequence $\mathbf{b}$. From (32) and (33), $L_c = l_w + 4 \le 2l + 4$ where l_w is a degree of $m_w(x)$.

In particular, if $\mathbf{a}$ is a binary m-sequence, then $m_a(x)$ is a primitive polynomial of degree l and thus we have $m_w(x) = m_a(x)$ or $(m_a(x))^2$ from (32). If $\eta \neq 0$, $\mathbf{w} \neq \mathbf{a}$ and thus $m_w(x) \neq m_a(x)$. Hence, $m_w(x) = (m_a(x))^2$ and consequently, $L_c = 2l + 4$ from (33). ■

REFERENCES

[1] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2934-2943, Nov. 2001.

[2] L. D. Baumert, *Cyclic Difference Sets*, Berlin, Springer-Verlag, 1971.

[3] E. R. Berlekamp. *Algebraic Coding Theory*. Aegean Park Press, CA, Revised ed. 1984.

[4] J. F. Dillon and H. Dobbertin, “New cyclic difference sets with Singer parameters,” *Finite Fields and Their Applications 10*, pp. 342-389, 2004.

[5] C. Ding, T. Helleseth, and K. Y. Lam, “Several classes of binary sequences with three-level autocorrelation,” *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2606-2612, Nov. 1999.

[6] C. Ding, T. Helleseth, and H. Martinsen, “New families of binary sequences with optimal three-valued autocorrelation,” *IEEE Trans. Inform. Theory*, vol. 47, no. 1, pp. 428-433, Jan. 2001.

[7] D. C. Chu, “Polyphase codes with periodic correlation properties,” *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 531-532, July 1972.

[8] R. L. Frank and S. A. Zadoff, “Phase shift pulse codes with good periodic correlation functions,” *IRE Trans. Inform. Theory*, vol. IT-8, pp. 381-382, Oct. 1962.

[9] S. W. Golomb, *Shift Register Sequences*, Holden-Day, Inc., San Francisco, 1967.

[10] S. W. Golomb and G. Gong, *Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar.* Cambridge University Press, 2005.

[11] G. Gong, “Theory and applications of q-ary interleaved sequences,” *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 400-411, Mar. 1995.

[12] G. Gong, “New designs for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ case,” *IEEE Trans. Inform. Theory*, vol. 48, no. 11, pp. 2847-2867, Nov. 2002.

[13] B. Gordon, W. H. Mills, and L. R. Welch, “Some new difference sets,” *Canadian J. Math.*, vol. 14, no. 4, pp. 614-625, 1962.

[14] T. Helleseth and P. V. Kumar, *Sequences with Low Correlation*, a chapter in *Handbook of Coding Theory*, edited by V. Pless and C. Huffmann, Elsevier Science Publishers, 1998.

[15] D. Jungnickel and A. Pott, “Difference sets: An introduction,” in *Difference Sets, Sequences and their Correlation Properties*, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds., 1999, vol. 542, NATO Science Series C, pp. 259-296.

[16] A. Lempel, M. Cohn, and W. Eastman, “A class of balanced binary sequences with optimal autocorrelation property,” *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 38-42, Jan. 1977.

[17] R. Lidl and H. Niederreiter, “Finite Fields,” in *Encyclopedia of Mathematics and Its Applications*, vol. 20, Reading, MA: Addison-Wesley, 1983.

[18] H. D. Lüke, “Sequences and arrays with perfect periodic correlation,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 24, no. 3, pp. 287-294, May 1988.

[19] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram, “Binary and quadriphase sequences with optimal autocorrelation properties: A survey,” *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 3271-3282, Dec. 2003.

[20] A. Maschietti, “Difference sets and hyperovals,” *Designs, Codes and Cryptography*, vol. 14, pp. 89-98, 1998.

[21] J. L. Massey, “Shift-register synthesis and BCH decoding,” *IEEE Trans. Inform. Theory*, vol. IT-15, no. 1, pp. 122-127, Jan. 1969.

[22] J. S. No, H. Chung, and M. S. Yun, “Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$,” *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 1278-1282, May 1998.

[23] J. -S. No, H. Chung, H. -Y. Song, K. Yang, J. -D. Lee, and T. Helleseth, “New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$,” *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1638-1644, May 2001.

[24] J. S. No, S. W. Golomb, G. Gong, H. K. Lee, and P. Gaal, “Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation,” *IEEE Trans. Inform. Theory*, vol.44, no. 2, pp. 814-817, Mar. 1998.

[25] V. M. Sidelnikov, “Some k-valued pseudo-random sequences and nearly equidistant codes,” *Probl. Inform. Transm.*, vol. 5, no. 1, pp. 12-16, 1969.

[26] B. Schmidt, “Cyclotomic integers and finite geometry,” *J. Amer. Math. Soc.*, vol. 12, pp. 929-952, 1999.

[27] Y. Zhang, J. G. Lei, and S. P. Zhang, “A new family of almost difference sets and some necessary conditions,” *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2052-2061, May 2006.