Information Sciences 287 (2014) 26–31

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

# A general construction of binary interleaved sequences of period 4N with optimal autocorrelation ☆

Tongjiang Yan [a,b,*], Zhixiong Chen [b,c], Bao Li [b]

[a] College of Sciences, China University of Petroleum, Qingdao 266555, China
[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100049, China
[c] Department of Mathematics, Putian University, Putian, Fujian 351100, China

ARTICLE INFO

*Article history:*
Received 21 February 2012
Received in revised form 8 June 2014
Accepted 24 July 2014
Available online 4 August 2014

*Keywords:*
Cryptography
Interleaved sequence
Optimal correlation
CDMA

ABSTRACT

A general construction of binary interleaved sequences of period 4N with low autocorrelation are considered in the paper. Firstly, some correlation properties of two general classes of binary interleaved sequences are presented. Secondly, based on these results, autocorrelation functions of a general construction of binary interleaved sequences of period 4N are given. Finally, we show that, from these results for general cases, several known binary sequences of these types with optimal autocorrelation and some other new binary sequences with low autocorrelation can be constructed.



## 1. Introduction

Pseudo-random sequences with low cross correlation can be employed in CDMA communications to combat interference from the other users who share a common channel and in stream cipher cryptosystems as key stream generators to resist cross-correlation attacks [5,2]. Given two binary sequences $\mathbf{a} = a(t)$ and $\mathbf{b} = b(t)$ of period $N$ over the binary field $F_2 = \{0, 1\}$, the periodic correlation of which is defined by

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

where the addition $t + \tau$ is performed modulo $N$. If $\mathbf{a} = \mathbf{b}$, $\Re_{\mathbf{a},\mathbf{b}}(\tau)$ is called the (periodic) autocorrelation function of $\mathbf{a}$, denoted by $\Re_{\mathbf{a}}(\tau)$, or simply $\Re(\tau)$ if the context is clear, otherwise, $\Re_{\mathbf{a},\mathbf{b}}(\tau)$ is called the (periodic) cross-correlation function of $\mathbf{a}$ and $\mathbf{b}$. Let $C_{\mathbf{a}} = \{0 \leqslant t \leqslant N-1 : a(t) = 1\}$ be the support of $\mathbf{a}$. Then

$$\Re_{\mathbf{a}}(\tau) = N - 4(|C_{\mathbf{a}}| - |(\tau + C_{\mathbf{a}}) \cap C_{\mathbf{a}}|), \tag{1}$$

where the symbol $||$ denotes the cardinality of a set [1]. From Eq. (1), the optimal values of out-of-phase autocorrelation of binary sequences in terms of the smallest possible values of the autocorrelation are classified into four types as follows: if

☆ This work is supported by the National Natural Science Foundations of China (No. 61170319), the Natural Science Fund of Shandong Province (No. ZR2010FM017), the Fundamental Research Funds for the Central Universities (No. 11CX04056A) and the China Postdoctoral Science Foundation funded project (No. 119103S148).

* Corresponding author at: College of Sciences, China University of Petroleum, Qingdao 266555, China.
*E-mail address:* yantoji@163.com (T. Yan).

http://dx.doi.org/10.1016/j.ins.2014.07.026
0020-0255/

$N \equiv 0 \bmod 4$, $R(\tau) \in \{0, -4, 4\}$; if $N \equiv 1 \bmod 4$, $R(\tau) \in \{1, -3\}$; if $N \equiv 2 \bmod 4$, $\Re(\tau) \in \{2, -2\}$; if $N \equiv 3 \bmod 4$, $\Re(\tau) = -1$ [10]. For the last case, $\Re(\tau)$ is often called ideal autocorrelation, which can guarantee that the sequence is balanced [4]. For more details about optimal autocorrelation, the reader is referred to [1,4]. In this paper, we will consider some binary sequences of period $4N$ with low autocorrelation, which can be constructed by the following interleaved technology.

**Definition 1** [3]. Fix two positive integers $T$ and $K$ where $T \geqslant 2$ and $K \geqslant 1$. Given a binary sequence $\mathbf{a} = (a(0), a(1), \ldots, a(K-1))$ of period $K$. If the binary sequence $\mathbf{u} = (u(0), u(1), \ldots, u(KT-1))$ can be given by an $K \times T$ matrix as follows:

$$\begin{bmatrix} u(0) & u(1) & \cdots & u(T-1) \\ u(T) & u(T+1) & \cdots & u(2T-1) \\ \vdots & & \vdots & \\ u((K-1)T) & u((K-1)T+1) & \cdots & u(KT-1) \end{bmatrix}, \tag{2}$$

which satisfies that each column of the matrix is a shift of $\mathbf{a}$ or an all-zero sequence, then $\mathbf{u}$ is called an interleaved sequence.

Let $\mathbf{u}_i$ be the $i$th column of the interleaved sequence $\mathbf{u}$. Then $\mathbf{u} = (\mathbf{u}_0, \ldots, \mathbf{u}_{T-1})$. With the development of interleaved technology, the above definition was generalized to the case that not all nonzero column vector $\mathbf{u}_j$ are required to be shift equivalent. For example, in [8], the case that $\mathbf{u}_j's$ are complement equivalent can be permitted. For more details about the interleaved construction, the reader is referred to [4]. In this paper, we use the generalized definition of interleaved sequences. For the original interleaved sequences, we call them classical interleaved sequences.

Assume the binary sequence $\mathbf{u} = (\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{T-1})$ possesses a $(K, T)$ interleaved construction, where each $\mathbf{u}_i$ is a binary column sequence of period $K$, and $L^\tau(\mathbf{u})$ denotes the left $\tau$-shift of $\mathbf{u}$.

**Lemma 1** [3]. *Let $\tau = \tau_1 T + \tau_2$, where $0 \leqslant \tau_2 \leqslant T-1$. The array form of $L^\tau(\mathbf{u})$ is given by*

$$(L^{k+\tau_1}(\boldsymbol{u}_{\tau_2}), \ldots, L^{k+\tau_1}(\boldsymbol{u}_{T-1}), L^{k+\tau_1+1}(\boldsymbol{u}_0), \ldots, L^{k+\tau_1+1}(\boldsymbol{u}_{\tau_2-1})). \tag{3}$$

In 2001, Arasu et al. gave a construction of binary sequences with optimal autocorrelation of period $4N$ by sequences with ideal autocorrelation of period $N \equiv 3 \bmod 4$ [1]. Then this construction was generalized in [9] and found to possess interleaved construction [8]. In 2010, Tang and Gong gave three new interleaved constructions of binary sequences with optimal autocorrelation values [6]. This paper will give more general constructions which can include them and some other new binary sequences with low autocorrelation.

## 2. Correlation properties of an interleaved sequence and its modification

**Definition 2.** A pair of binary sequences $\mathbf{s}$ and $\mathbf{s}'$ by

$$\mathbf{s} = (\mathbf{0}_K, \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{T-1}), \quad \mathbf{s}' = (\mathbf{1}_K, \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{T-1}),$$

where $\mathbf{0}_K$ is an all-zero sequence and $\mathbf{1}_K$ is an all-one sequence of period $K$, $\mathbf{a}_i's$ are binary sequences of period $K$.

The balance difference of each $\mathbf{a}_i$ is given as $d(\mathbf{a}_i) = 2|C_{\mathbf{a}_i}| - K$.

In [6], generalized GMW sequences and their modifications of period $2^{2n}-1$ are defined respectively as the above sequences $\mathbf{s}$ and $\mathbf{s}'$ with an additional condition that all $\mathbf{a}_i's$ are some shifts of an ideal autocorrelation sequence $\mathbf{a}$. Then $d(\mathbf{a}_i)$ is constant and takes value 1 or $-1$. If $d(\mathbf{a}_i) = -1$, we can get a pair of modified sequences $\bar{\mathbf{s}}$ and $\bar{\mathbf{s}}'$ by replacing each $\mathbf{a}_i$ with its complement sequence, and keep their autocorrelation unchanged [4]. So we may assume that each $d(\mathbf{a}_i)$ always takes the value 1 when $\mathbf{s}$ and $\mathbf{s}'$ are generalized GMW sequences and their modifications respectively [3].

The sequence $\mathbf{s}$ and its modification $\mathbf{s}'$ have the following properties of correlation.

**Theorem 1.** *Let $\tau = \tau_1 T + \tau_2$, $0 \leqslant \tau_2 \leqslant T-1$. The autocorrelation of $\mathbf{s}'$ is given by*

$$\Re_{\mathbf{s}'}(\tau) = \begin{cases} \Re_{\mathbf{s}}(\tau) & \text{if } \tau_2 = 0, \\ \Re_{\mathbf{s}}(\tau) + 2d(\boldsymbol{a}_{\tau_2}) + 2d(\boldsymbol{a}_{T-\tau_2}) & \text{if } \tau_2 \neq 0. \end{cases}$$

*The cross-correlation of $\mathbf{s}$ and $\mathbf{s}'$ is given by*

$$\Re_{\mathbf{s}\mathbf{s}'}(\tau) = \begin{cases} TK - 2K & \text{if } \tau = 0, \\ \Re_{\mathbf{s}}(\tau) - 2K & \text{if } \tau_2 = 0,\ \tau \neq 0, \\ \Re_{\mathbf{s}}(\tau) + 2d(\boldsymbol{a}_{T-\tau_2}) & \text{otherwise}, \end{cases}$$

$$\Re_{\mathbf{s}'\mathbf{s}}(\tau) = \begin{cases} KT - 2K & \text{if } \tau = 0, \\ \Re_{\mathbf{s}}(\tau) - 2K & \text{if } \tau_2 = 0,\ \tau \neq 0, \\ \Re_{\mathbf{s}}(\tau) + 2d(\boldsymbol{a}_{\tau_2}) & \text{otherwise}. \end{cases}$$