New Classes of Balanced Quaternary and Almost Balanced Binary Sequences With Optimal Autocorrelation Value

Xiaohu Tang, *Member, IEEE*, and Cunsheng Ding, *Senior Member, IEEE*

***Abstract*—Sequences with optimal autocorrelation property are needed in certain communication systems and cryptography. In this paper, a construction of balanced quaternary sequences with period $N \equiv 2 (\mathrm{mod}\ 4)$ and optimal autocorrelation value and a construction of almost balanced binary sequences with period $N \equiv 0 (\mathrm{mod}\ 4)$ and optimal autocorrelation value are presented. Both constructions are a generalization of earlier ones.**

***Index Terms*—Almost balance, balance, binary sequence, optimal autocorrelation, quaternary sequence.**

I. Introduction

LET $a = (a(t), t = 0, \ldots, N-1)$ be a sequence of period N over $\mathbf{Z}_m = \{0, \ldots, m-1\}$. For any $0 \le k < m$, define $N_k(a) = |\{0 \le t < N : a(t) = k\}|$. Then a is said to be *balanced* if $\max_{k \in \mathbf{Z}_m} N_k(a) - \min_{k \in \mathbf{Z}_m} N_k(a) = 0$ for $N \equiv 0 (\mathrm{mod}\ m)$ and $\max_{k \in \mathbf{Z}_m} N_k(a) - \min_{k \in \mathbf{Z}_m} N_k(a) = 1$ for $N \not\equiv 0 (\mathrm{mod}\ m)$. This paper deals mainly with two types of balanced sequences: binary (i.e., $m = 2$) sequences and quaternary (i.e., $m = 4$) sequences. In addition, *almost balanced* binary sequences are investigated as well, which are defined by $N_0(a) = \frac{N}{2} \pm 1$ for even N and $N_0(a) = \frac{N \pm 1}{2}$ for odd N.

Given two sequences $a = (a(t), t = 0, \ldots, N-1)$ and $b = (b(t), t = 0, \ldots, N-1)$ of period N over $\mathbf{Z}_m$, the *periodic correlation* function between a and b at the shift $0 \le \tau < N$ is defined as

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

where $\omega = e^{\frac{2\pi\sqrt{-1}}{m}}$ is the complex primitive mth root of unity.

If $a = L^\tau(b)$ for an integer $0 \le \tau < N$, where L is the left cyclic shift operator, i.e., $L^\tau(b) = (b(\tau), \ldots, b(\tau + N - 1))$ in which the addition $t + \tau$ is performed modulo N, $R_{a,b}$ is called the *autocorrelation* of a, denoted by R_a or simply R if the context is clear. Otherwise, $R_{a,b}$ is called the *cross-correlation* of a and b.

For applications in direct-sequence code-division multiple access, coding theory and cryptography, balanced or almost balanced sequences with good autocorrelation property are preferred as balanceness and good autocorrelation are two measures of randomness for sequences. In the literature, a binary sequence a is said having optimal autocorrelation property if it satisfies one or two of the following conditions:

P1. The maximal out-of-phase autocorrelation magnitude is as small as possible.

P2. The number of occurrences of the maximal out-of-phase autocorrelation magnitude is as small as possible.

If the sequence a satisfies Condition P1, then it is referred to as a sequence with the optimal autocorrelation magnitude. Further, a is said to be a sequence with optimal autocorrelation value if it also satisfies Condition P2.

For almost balanced or balanced binary sequences of period N, the optimal autocorrelation values are classified into four types as follows according to the remainder of N modulo 4 [1]:

A) $R(\tau) \in \{0, -4\}$ if $N \equiv 0 (\mathrm{mod}\ 4)$;

B) $R(\tau) \in \{1, -3\}$ if $N \equiv 1 (\mathrm{mod}\ 4)$;

C) $R(\tau) \in \{2, -2\}$ if $N \equiv 2 (\mathrm{mod}\ 4)$; and

D) $R(\tau) = -1$ if $N \equiv 3 (\mathrm{mod}\ 4)$;

where $0 < \tau < N$. In [1], [4], [5], [7], and [14], a number of constructions of binary sequences with optimal autocorrelation value have been developed. When $N \equiv 0 (\mathrm{mod}\ 4)$, classes of binary sequences with optimal autocorrelation magnitude, i.e., $R(\tau) \in \{0, \pm 4\}$, were proposed in [16] and [17].

Known results about quaternary sequences with optimal or best known autocorrelation were discussed in the survey paper [14]. But balanced quaternary sequences with optimal autocorrelation property seemed unknown until the constructions of balanced quaternary sequences of period $N \equiv 2 (\mathrm{mod}\ 4)$ or $N \equiv 0 (\mathrm{mod}\ 4)$ were presented very recently [8], [11], [12]. According to the aforementioned definition, we will see in Section IV that the sequences of period $N \equiv 2 (\mathrm{mod}\ 4)$ in [8], [11] have optimal autocorrelation value and the sequences of period $N \equiv 0 (\mathrm{mod}\ 4)$ in [12] possess optimal autocorrelation magnitude.

In this paper, we mainly investigate balanced quaternary sequences of period $N \equiv 2 (\mathrm{mod}\ 4)$ with optimal autocorrelation value. The first objective of this paper is to determine their exact out-of-phase autocorrelation values. The second one is to present a new family of balanced quaternary sequences of period $N \equiv 2 (\mathrm{mod}\ 4)$ with optimal autocorrelation values, which

Manuscript received September 13, 2009. Date of current version November 19, 2010. The work of X. H. Tang was supported by the National Science Foundation of China (NSFC) under Grant 60772086.

X. H. Tang is with the Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, Sichuan 610031, China (e-mail: xhutang@ieee.org).

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong (e-mail: cding@ust.hk).

Communicated by M. G. Parker, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2010.2081170

is a generalization of the construction in [8]. Additionally, applying the Gray mapping to the proposed quaternary sequences, a new family of almost balanced binary sequences of period $N \equiv 0 (\bmod\, 4)$ with optimal autocorrelation value is obtained, which generalizes the known constructions in [1] and [16].

II. Preliminaries

A. Interleaved Structure

In [6], Gong introduced the $N \times T$ interleaved structure of sequences. Let $\{a_0, a_1, \ldots, a_{T-1}\}$ be a sequence set consisting of T sequences of period N, $a_i = (a_i(t), t = 0, \ldots, N-1)$, $0 \le i < T$. An $N \times T$ matrix is formed by placing the sequence a_i on the ith column $0 \le i < T$, i.e.

$$U = [a_0, a_1, \ldots, a_{T-1}].$$

Concatenating the successive rows of matrix U, one can obtain an interleaved sequence u of period NT. For short, we write the interleaved sequence u as

$$u = I(a_0, a_1, \ldots, a_{T-1}) \quad (1)$$

where I is the interleaving operator, and call $\{a_0, a_1, \ldots, a_{T-1}\}$ the column sequences of u.

Let $v = I(b_0, b_1, \ldots, b_{T-1})$ be another interleaved sequence constructed from the column sequences $\{b_0, b_1, \ldots, b_{T-1}\}$, $b_i = (b_i(t), t = 0, \ldots, N-1)$, $0 \le i < T$. Consider its left cyclical shift version $L^\tau(v)$, where $\tau = T\tau_1 + \tau_2$ $(0 \le \tau_1 < N$, $0 \le \tau_2 < T)$. It was shown that $L^\tau(v)$ is just another interleaved sequence [6]. Namely, we have

$$\begin{aligned} L^\tau(v) = I(L^{\tau_1}(b_{\tau_2}), \ldots, L^{\tau_1}(b_{T-1}) \\ L^{\tau_1+1}(b_0), \ldots, L^{\tau_1+1}(b_{\tau_2-1})). \quad (2) \end{aligned}$$

Then, the correlation function between the interleaved sequences u and v at the shift τ becomes the summation of the inner products between the pairwise column sequences in (1) and (2), i.e.

$$\begin{aligned} R_{u,v}(\tau) = &\sum_{i=0}^{T-\tau_2-1} R_{a_i, b_{i+\tau_2}}(\tau_1) \\ &+ \sum_{i=T-\tau_2}^{T-1} R_{a_i, b_{i+\tau_2-T}}(\tau_1 + 1). \quad (3) \end{aligned}$$

In Sections V–VI, we will, respectively, use the $N \times 2$ and $N \times 4$ interleaved structures to design quaternary sequences and binary sequences with optimal autocorrelation value.

B. Gray Mapping and Its Inverse

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

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

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

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

any quaternary sequence $u = (u(t), t = 0, \ldots, N-1)$ can be obtained from two binary sequences $a = (a(t), t = 0, \ldots, N-1)$ and $b = (b(t), t = 0, \ldots, N-1)$ of the same period N as follows:

$$u(t) = \phi^{-1}(a(t), b(t)), \quad 0 \le t < N.$$

Transforming the sequence u into its complex valued version, i.e.

$$\omega^{u(t)} = \frac{1}{2}(1+\omega)(-1)^{a(t)} + \frac{1}{2}(1-\omega)(-1)^{b(t)}, 0 \le t < N$$

where $\omega = \sqrt{-1}$, Krone and Sarwate observed the following relation between their correlations.

Lemma 1 ([13]): The autocorrelation function of u is given by

$$R_u(\tau) = \frac{1}{2}[R_a(\tau) + R_b(\tau)] + \frac{\omega}{2}[R_{a,b}(\tau) - R_{b,a}(\tau)].$$

C. Binary Ideal Sequences

When $N \equiv 3 (\bmod\, 4)$, binary sequences of Type D are called *ideal* sequences. According to the format of the period N, the known ideal sequences can be divided into the following four classes [7].

1) $N = 2^n - 1$, n positive integer: there are four kinds of such sequences, i.e., (a) m-sequences; (b) Kasami power function class or the B_k class of Dillon and Dobbertin; (c) Welch-Gong (WG) transform sequences; and (d) GMW and generalized GMW sequences with those sequences as a decomposition;
2) $N = p$, p a prime: Legendre sequences;
3) $N = p(p+2)$, both p and $p+2$ are primes: twin-prime sequences; and
4) $N = 4k^2 + 27$: Hall sequences.

D. The Two Types of Legendre Sequences

The Legendre sequence $l = (l(t), t = 0, \ldots, N-1)$ of period N, N odd prime, is defined as

$$l(i) = \begin{cases} 0 \text{ or } 1, & \text{if } i = 0 \\ 1, & \text{if } i \in \mathbf{QR}_N \\ 0, & \text{if } i \in \mathbf{NQR}_N \end{cases}$$

where $\mathbf{QR}_N$ and $\mathbf{NQR}_N$ are the set of quadratic residues and quadratic nonresidues modulo N. In particular, l is called the *first type* Legendre sequence if $l(0) = 1$ otherwise the *second type* Legendre sequence in this paper.

It is well known that Legendre sequences have optimal autocorrelation value if $N = 3(\bmod 4)$ or $N = 1(\bmod 4)$.

III. Combinatorial Characterizations of Binary Sequences With Optimal Autocorrelation Value

Let $a = (a(t), t = 0, \ldots, N-1)$ be a binary sequence of period N. We say that

$$C_a = \{0 \le t < N : a(t) = 1\}$$

is the *support* of the sequence a. To characterize the support of the binary sequence with optimal autocorrelation value, we need to introduce difference sets and almost difference sets.

Let $(G,+)$ be an abelian group of order N. Let A be a k-subset of G. The set A is an (N,k,λ) *difference set* (DS) in G if the difference function

$$d_A(\tau) := |(A+\tau)\cap A| = \lambda$$

for every nonzero element τ of G, where $A+\tau = \{a+\tau : a\in A\}$. The reader is referred to [9] and [10] for the detailed information of difference sets.

A k-subset A of G is an (N,k,λ,t) *almost difference set* (ADS) in G if $d_A(\tau)$ takes on λ altogether t times and $\lambda+1$ altogether $N-1-t$ times when τ ranges over all the nonzero elements of G [1].

The balanced or almost balanced binary sequences of period N with optimal autocorrelation value are characterized by the following [1].

Theorem 2: Let $(a(t), t=0,\ldots,N-1)$ be a binary sequence of period N, and let C_a be its support.

1) Let $N\equiv 0 (\mathrm{mod}\ 4)$. Then $R_a(\tau)\in\{0,-4\}$ for all $\tau \not\equiv 0 (\mathrm{mod}\ N)$ iff C_a is an $(N,k,k-(N+4)/4, Nk-k^2-(N-1)N/4)$ ADS in $\mathbf{Z}_N$, where $k=N/2$ if a is balanced, and $k=N/2-1$ or $N/2+1$ if a is almost balanced.
2) Let $N\equiv 1 (\mathrm{mod}\ 4)$. Then $R_a(\tau)\in\{1,-3\}$ for all $\tau\not\equiv 0(\mathrm{mod}\ N)$ iff C_a is an $(N,(N+1)/2,k-(N+3)/4,Nk-k^2-(N-1)^2/4)$ ADS in $\mathbf{Z}_N$, where $k=(N-1)/2$ or $(N+1)/2$ if a is balanced, and $k=(N+3)/2$ or $(N-3)/2$ if a is almost balanced.
3) Let $N\equiv 2 (\mathrm{mod}\ 4)$. Then $R_a(\tau)\in\{2,-2\}$ for all $\tau\not\equiv 0(\mathrm{mod}\ N)$ iff C_a is an $(N,k,k-(N+2)/4,Nk-k^2-(N-1)(N-2)/4)$ ADS in $\mathbf{Z}_N$, where $k=N/2$ if a is balanced, and $k=N/2-1$ or $N/2+1$ if a is almost balanced.
4) Let $N\equiv 3 (\mathrm{mod}\ 4)$. Then $R_a(\tau)=-1$ for all $\tau\not\equiv 0(\mathrm{mod}\ N)$ iff C_a is an $(N,(N-1)/2,(N-3)/4)$ or $(N,(N+1)/2,(N+1)/4)$ DS in $\mathbf{Z}_N$.

IV. Balanced Quaternary Sequences of Period $N\equiv 0(\mathrm{mod}\ 2)$ With Optimal Autocorrelation Property

Let $u=(u(t), t=0,\ldots,N-1)$ be a quaternary sequence of period N. Given $0<\tau<N$, denote by $n_0(u,\tau), n_1(u,\tau), n_2(u,\tau)$ and $n_3(u,\tau)$ the number of occurrence of 0,1,2, and 3 in the difference $u(t)-u(t+\tau)(\mathrm{mod}\ 4)$ with t ranging over $\mathbf{Z}_N$. Then, the autocorrelation of u can be rewritten as

$$R_u(\tau) = n_0(u,\tau)-n_2(u,\tau)+\omega(n_1(u,\tau)-n_3(u,\tau)). \quad (4)$$

It is seen from (4) that the best case is the perfect autocorrelation, i.e., $R_a(\tau)=0$ for all $0<\tau<N$. Such a sequence is called *perfect*. However, only quaternary perfect sequences of period 2, 4, 8, and 16 are found [14]. It is proved there does not exist a perfect quaternary sequence of period 2^k for $k>4$ [3]. It is known that the existence of a perfect quaternary sequence is equivalent to that of a complex circulant Hadamard matrix. It is conjectured in [2] that there does not exist such a matrix of order more than 16. It is equivalently conjectured that there does not exist a perfect quaternary sequence of period more than 16 [15]. Parraud obtained some necessary conditions on the existence of perfect quaternary sequences [15]. In spite of the efforts made by the community, the existence problem of perfect quaternary sequences remains open.

Our first contribution in this paper is the following.

Lemma 3: There is no balanced perfect quaternary sequence of period N with $N>2$.

Proof: Suppose that u is a perfect quaternary sequence of period N. Then by definition $R_u(\tau)=0$ for all τ with $0<\tau<N$. Hence

$$\sum_{\tau=0}^{N-1} R_u(\tau) = N.$$

On the other hand, we have that

$$\begin{aligned}\sum_{\tau=0}^{N-1} R_u(\tau) &= \sum_{\tau=0}^{N-1}\sum_{t=0}^{N-1}\omega^{u(t)-u(t+\tau)}\\ &= \sum_{t=0}^{N-1}\omega^{u(t)}\sum_{\tau=0}^{N-1}\omega^{-u(t+\tau)}\\ &= \left(\sum_{t=0}^{N-1}\omega^{u(t)}\right)\left(\sum_{\tau=0}^{N-1}\omega^{-u(\tau)}\right)\\ &= \left|\sum_{t=0}^{N-1}\omega^{u(t)}\right|^2\\ &= |N_0(u)-N_2(u)+\omega(N_1(u)-N_3(u))|^2\\ &= (N_0(u)-N_2(u))^2+(N_1(u)-N_3(u))^2.\end{aligned} \quad (5)$$

It follows that

$$N=(N_0(u)-N_2(u))^2+(N_1(u)-N_3(u))^2.$$

Hence, we obtain

$$\begin{aligned}\sqrt{N/2} &\le \max\{|N_0(u)-N_2(u)|, |N_1(u)-N_3(u)|\}\\ &\le \max_{i\in\mathbf{Z}_4} N_i(u) - \min_{i\in\mathbf{Z}_4} N_i(u).\end{aligned} \quad (6)$$

As defined in the introductory section, u is balanced if $\max_{i\in\mathbf{Z}_4} N_i(u)-\min_{i\in\mathbf{Z}_4} N_i(u)\le 1$. The conclusion of this lemma then follows from (6). ■

It is noticed that the proof of Lemma 3 proved a much stronger result.

Lemma 4: The maximum out-of-phase autocorrelation magnitude of any balanced quaternary sequence u of period $N\equiv 0(\mathrm{mod}\ 2)>2$ is at least 2.

Proof: Note that

$$\begin{aligned}&|R_u(\tau)|\\ &\quad = \sqrt{(n_0(u,\tau)-n_2(u,\tau))^2+(n_1(u,\tau)-n_3(u,\tau))^2}.\end{aligned} \quad (7)$$

First, we prove that $n_0(u,\tau)-n_2(u,\tau)$ is even. Suppose that $u(t)=\phi^{-1}(a(t),b(t))$. Then by Lemma 1,

$$\Re(R_u(\tau)) = \frac{1}{2}[R_a(\tau)+R_b(\tau)]$$

where $\Re(x)$ denotes the real part of the complex-valued variable x.

For any binary sequences $a = (a(t), t = 0, \ldots, N-1)$ and $b = (b(t), t = 0, \ldots, N-1)$, it is well known that [5]

$$R_a(\tau) = N - 4k_1,\ R_b(\tau) = N - 4k_2$$

for some integers k_1 and k_2. So

$$\begin{aligned} n_0(u,\tau) - n_2(u,\tau) &= \Re(R_u(\tau)) \\ &= \frac{1}{2}[2N - 4(k_1 + k_2)] \\ &= N - 2(k_1 + k_2). \end{aligned}$$

Immediately, $n_0(u,\tau) + n_2(u,\tau) = (n_0(u,\tau) - n_2(u,\tau)) + 2n_2(u,\tau)$ is also even. It then follows from $n_0(u,\tau) + n_1(u,\tau) + n_2(u,\tau) + n_3(u,\tau) = N$ that $n_1(u,\tau) + n_3(u,\tau)$ is even. Hence, $n_1(u,\tau) - n_3(u,\tau)$ is even as well.

If $|R_u(\tau)| \neq 0$, then by (7) we have $|R_u(\tau)| \geq 2$. The conclusion of this lemma then follows from Lemma 3. ■

Let u be a balanced quaternary sequence of period $N \equiv 0 (\bmod 2)$. According to Lemma 4, we have

$$\max_{0<\tau<N} |R_u(\tau)| \geq 2.$$

When the equality holds, the possible out-of-phase autocorrelation values $R_u(\tau)$ are in $\{0, \pm 2, \pm 2\omega\}$. Assume that $R_u(\tau)$ takes on each $x \in \{\pm 2, \pm 2\omega\}$ exactly Γ_x times when τ ranges over $0 < \tau < N$. It then follows from (5) that

$$2\Gamma_2 - 2\Gamma_{-2} + \omega(2\Gamma_{2\omega} - 2\Gamma_{-2\omega}) = C$$

where $C = -N$ or $-N+2$ is a constant, which depends on $|\sum_{t=0}^{N-1} \omega^{u(t)}|^2 = 0$ or 2 for $N \equiv 2 (\bmod 4)$ and $|\sum_{t=0}^{N-1} \omega^{u(t)}|^2 = 0$ for $N \equiv 0 (\bmod 4)$. We then have $\Gamma_{2\omega} = \Gamma_{-2\omega}$ and

$$2\Gamma_2 - 2\Gamma_{-2} = C$$

which implies that

$$2\Gamma_{-2} \geq -C \tag{8}$$

and the equality holds if and only if $\Gamma_2 = 0$.

The number of occurrence of the magnitude 2 in the multiset $\{|R_u(\tau)| : 0 < \tau < N\}$ is

$$\begin{aligned} \Delta &= \Gamma_2 + \Gamma_{2\omega} + \Gamma_{-2} + \Gamma_{-2\omega} \\ &\geq \Gamma_{-2} \\ &\geq \frac{-C}{2} \end{aligned}$$

where the last inequality follows from (8). We then conclude that $\Delta = -C/2$ is minimal iff $R_u(\tau) \in \{0, -2\}$ for all τ with $0 < \tau < N$.

Because balanced quaternary sequences of period $N \equiv 2 (\bmod 4)$ with nontrivial autocorrelation $\{0, -2\}$ and those of period $N \equiv 0 (\bmod 4)$ with nontrivial autocorrelation $\{-2, \pm 2\omega\}$ have been presented in [8], [11], and [12], we have the following definitions for balanced quaternary sequences with optimal autocorrelation property.

Definition 1: When $N \equiv 0 (\bmod 2)$, a balanced quaternary sequence u of period N is said having optimal autocorrelation magnitude if $|R_u(\tau)| \leq 2$ for all $0 < \tau < N$.

Definition 2: When $N \equiv 2 (\bmod 4)$, a balanced quaternary sequence u of period N is said having optimal autocorrelation value if $R_u(\tau) \in \{0, -2\}$ for all $0 < \tau < N$.

In the next section we will construct a large family of balanced quaternary sequences of period $N \equiv 2 (\bmod 4)$ with optimal autocorrelation value.

Remark 1: By Definition 2, the sequences in [8] and [11] are balanced quaternary sequences of period $N \equiv 2 (\bmod 4)$ with optimal autocorrelation value. While according to Definition 1, the balanced sequence v of period $N \equiv 0 (\bmod 4)$ in [12] has optimal autocorrelation magnitude. However, it still needs to be further investigated whether v has optimal autocorrelation value. In other words, it is still open if $R_v(\tau) = 0$ for some $0 < \tau < N$ is possible for a balanced quaternary sequence v of period $N \equiv 0 (\bmod 4)$ with optimal autocorrelation magnitude.

V. The Construction of Quaternary Sequences With Optimal Autocorrelation Value From Ideal Sequences

Construction A: Let $N \equiv 3 (\bmod 4)$. Let $a = (a(t), t = 0, \ldots, N-1)$ and $b = (b(t), t = 0, \ldots, N-1)$ be two binary ideal sequences of period N. The construction consists of the following two steps:

1) Generate two binary sequences c and d of period $2N$ as

$$c = I\left(a, L^{(N+1)/2}(a)\right) \tag{9}$$

$$d = I(b, L^{(N+1)/2}(b) + 1) \tag{10}$$

where $L^{(N+1)/2}(b) + 1$ denotes the sequence $(b(t + (N+1)/2) + 1, t = 0, \ldots, N-1)$, in which the addition $b(t + (N+1)/2) + 1$ is computed modulo 2.

2) Construct a quaternary sequence u of period $2N$ as

$$u = \phi^{-1}(c, d), \tag{11}$$

where ϕ^{-1} is the inverse Gray mapping.

Let us now look at the matrix expression U, C, and D of the sequences u, c, and d, respectively, say

$$\begin{aligned} U &= (U_{i,j})_{0 \leq i < N, 0 \leq j < 2} \\ C &= (C_{i,j})_{0 \leq i < N, 0 \leq j < 2} \\ D &= (D_{i,j})_{0 \leq i < N, 0 \leq j < 2}. \end{aligned}$$

Suppose $U_{i,0} = 0$ (respectively, $U_{i,0} = 1$) for some i with $0 \leq i < N$. By the Gray mapping, $(C_{i,0}, D_{i,0}) = (0,0)$ (respectively, $(C_{i,0}, D_{i,0}) = (0,1)$). From the construction of the sequences c and d in (9) and (10), we know $(C_{i+(N+1)/2,1}, D_{i+(N+1)/2,1}) = (0,1)$ (respectively, $(C_{i+(N+1)/2,1}, D_{i+(N+1)/2,1}) = (0,0)$), i.e., $U_{i+(N+1)/2,1} = 1$ (respectively, $U_{i+(N+1)/2,1} = 0$), where the addition of the subscripts is reduced modulo N. The converse deduction holds as well. Then, we conclude that

$N_0(u) = N_1(u) = N_0(a)$, which is equal to $\frac{N-1}{2}$ or $\frac{N+1}{2}$, the number of occurrence of 0 in a periodic segment of the ideal sequence a.

If $U_{i,0} = 2$ or $U_{i,0} = 3$ for some i, similar arguments will lead to $N_2(u) = N_3(u) = N_1(a) = \frac{N+1}{2}$ or $\frac{N-1}{2}$. Therefore, the sequence u is balanced. This proved the following theorem.

Theorem 5: The sequence u constructed by (11) is balanced, i.e.

$$N_0(u) = N_1(u) = \frac{N-1}{2}, N_2(u) = N_3(u) = \frac{N+1}{2}$$

or

$$N_0(u) = N_1(u) = \frac{N+1}{2}, N_2(u) = N_3(u) = \frac{N-1}{2}.$$

Now we show that the balanced quaternary sequence u has the optimal autocorrelation value.

Theorem 6: The sequence u constructed by (11) is a balanced quaternary sequence of period $2N$ with optimal autocorrelation value, and in particular,

$$R_u(\tau) = \begin{cases} 2N, & 1 \text{ time} \\ 0, & N \text{ times} \\ -2, & N-1 \text{ times.} \end{cases}$$

Proof: By Lemma 1

$$\begin{aligned} R_u(\tau) &= \frac{1}{2}[R_c(\tau) + R_d(\tau)] + \frac{\omega}{2}[R_{c,d}(\tau) - R_{d,c}(\tau)] \\ &= \frac{1}{2}[R_c(\tau) + R_d(\tau)] + \frac{\omega}{2}[R_{c,d}(\tau) - R_{c,d}(-\tau)] \end{aligned} \tag{12}$$

where the second identity comes from the simple fact that $R_{c,d}(\tau) = R_{d,c}(-\tau)$ for any two sequences c and d.

Given $\tau = 2\tau_1 + \tau_2$, ($0 < \tau_1 < N$ and $\tau_2 = 0$) or ($0 \le \tau_1 < N$ and $\tau_2 = 1$), there are two cases to discuss the autocorrelation of u.

Case 1. $\tau_2 = 0$.

For this case, $0 < \tau_1 < N$. Applying (3) to the $N \times 2$ interleaved structure of the sequences c and d, we get

$$\begin{aligned} R_c(\tau) &= R_a(\tau_1) + R_a(\tau_1) = -2, \\ R_d(\tau) &= R_b(\tau_1) + R_b(\tau_1) = -2 \end{aligned}$$

which follows from the ideal autocorrelation property of the sequences a and b, and

$$R_{c,d}(\tau) = R_{a,b}(\tau_1) - R_{a,b}(\tau_1) = 0.$$

Substituting them into (12), we obtain $R_u(\tau) = -2$.

Case 2. $\tau_2 = 1$.

Applying (3) to the sequences c and d in place of $T = 2$ and $\tau_2 = 1$, we have

$$\begin{aligned} R_c(\tau) &= R_a\left(\tau_1 + \frac{N+1}{2}\right) + R_a\left(\tau_1 + \frac{N+1}{2}\right) \\ &= \begin{cases} 2N, & \text{if } \tau_1 = \frac{N-1}{2} \\ -2, & \text{else,} \end{cases} \end{aligned}$$

$$\begin{aligned} R_d(\tau) &= -R_b\left(\tau_1 + \frac{N+1}{2}\right) - R_b\left(\tau_1 + \frac{N+1}{2}\right) \\ &= \begin{cases} -2N, & \text{if } \tau_1 = \frac{N-1}{2} \\ 2, & \text{else} \end{cases} \end{aligned}$$

in which we made use of $\tau_1 + 1 - \frac{N+1}{2} = \tau_1 + \frac{N+1}{2} (\text{mod } N)$ and the ideal autocorrelation property of the sequences a and b again.

Again applying (3) to the calculation of the cross-correlation $R_{c,d}(\tau)$, it results in

$$\begin{aligned} R_{c,d}(\tau) = &-R_{a,b}\left(\tau_1 + \frac{N+1}{2}\right) + R_{a,b}\left(\tau_1 + \frac{N+1}{2}\right) \\ = &\ 0. \end{aligned}$$

Therefore, we have $R_u(\tau) = 0$.

Summarizing the two cases above, we have proved the optimal autocorrelation property of the balanced quaternary sequence u. ■

Example 1: Let a be the binary m-sequence of period 7 given by

$$a = (0, 0, 1, 0, 1, 1, 1)$$

and b be its 3-decimated version, i.e.

$$b = (0, 0, 1, 1, 1, 0, 1)$$

where $b(t) = a(3t \bmod 7)$ for all $t \ge 0$. Then by Construction A, a balanced quaternary sequence of period 14 is generated as

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

It is easily checked that u has optimal autocorrelation value

$$\begin{aligned} &(R_u(\tau))_{\tau=0}^{13} \\ &\qquad = (14, 0, -2, 0, -2, 0, -2, 0, -2, 0, -2, 0, -2, 0). \end{aligned}$$

Example 2: Let $N = 31$, and let a and b be the Hall sequence defined by the primitive root 3 and the Legendre sequence of the same period 31. Then

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

and $N_0(u) = N_1(u) = 16$ and $N_2(u) = N_3(u) = 15$. We have also that $R_u(\tau) = 0$ if τ is an odd integer between 1 and 61 and $R_u(\tau) = -2$ if τ is an even integer between 1 and 61.

Remark 2: Note that in Construction A, a and b can be any two ideal sequences of the same period. It is possible that a and

b are the equivalent ideal sequence with respect to the shift operation, i.e., $b = L^{\tau}(a)$ for an integer $0 \leq \tau < N$. In particular, when $\tau = 0$ and $b = a$, the u constructed in this section becomes the balanced quaternary sequence q with optimal autocorrelation value proposed in Theorem 3 in [8]. In the following, we show that the sequence q constructed in [8] is just a product sequence.

Write $q = I(q_0, L^{\frac{N+1}{2}}(q_1))$. Then by Construction A

$$q_0 = \phi^{-1}(a, a), q_1 = \phi^{-1}(a, a+1).$$

Let $q_0(t)$ and $q_1(t)$ be the tth entry of the sequence q_0 and q_1, respectively. According to the inverse Gray mapping, the relation among $a(t)$, $q_0(t)$, and $q_1(t)$ are listed in the following table:

$a(t)$	$a(t)+1$	$q_0(t)$	$q_1(t)$
(mod 2)	(mod 2)	(mod 4)	(mod 4)
0	1	0	1
1	0	2	3

So, we have that $q_0 = 2a$ and $q_1 = 2a + 1$, i.e.

$$q = I(2a, L^{\frac{N+1}{2}}(2a) + 1)$$

where $2a$ denotes the sequence $(2a(t), t = 0, \ldots, N-1)$. That is

$$\begin{aligned} q = \Big(& 2a(0), 2a\left(\frac{N+1}{2}\right) + 1, 2a(1), \\ & 2a\left(\frac{N+1}{2} + 1\right) + 1, \ldots, \\ & 2a(N-1), 2a\left(\frac{N+1}{2} + N - 1\right) + 1\Big) \end{aligned}$$

is a product sequence of the sequence

$$\left(2a(0), 2a\left(\frac{N+1}{2}\right), \ldots, 2a\left(\frac{N-1}{2}\right)\right)$$

and the sequence $(0, 1)$, where the former is the $\frac{N+1}{2}$-decimated version of the sequence $2a$, i.e., the sequence $(2a(\frac{N+1}{2}t \bmod N))$, and the later is a prefect quaternary sequence of period 2.

In fact, the sequence in [11], denoted by s here, is the one bit modification of the above product sequence by letting a be the Legendre sequence, more precisely

$$s = I\left(2l, L^{\frac{N+1}{2}}(2l') + 1\right)$$

where l and l' are, respectively, the first type and the second type of Legendre sequence of period N (N odd prime). It should be noted that the ideal autocorrelation property is not needed for the Legendre sequence for this case, i.e., the period N can be an odd prime with $N \equiv 1 (\bmod 4)$.

In summary, the construction of this section is indeed a generalization of the one presented in [8].

VI. The Construction of Binary Sequences With Optimal Autocorrelation Value From Ideal Sequences

Construction B: Let $N \equiv 3 (\bmod 4)$. Let $a = (a(t), t = 0, \ldots, N-1)$ and $b = (b(t), t = 0, \ldots, N-1)$ be two binary ideal sequences of period N. A new binary sequence of period $4N$ is constructed by

$$w = I\left(a, L^{\frac{N+1}{4}}(b), L^{\frac{N+1}{2}}(a), L^{\frac{3(N+1)}{4}}(b) + 1\right). \quad (13)$$

Remark 3: Actually, the binary sequence w in (13) is a modification of the Gray mapping sequence of the quaternary sequence u defined by (11). First performing the Gray mapping on u in (11), we obtain a binary sequence

$$w' = I(a, b, L^{\frac{N+1}{2}}(a), L^{\frac{N+1}{2}}(b) + 1).$$

Next, shifting the column sequences b and $L^{\frac{N+1}{2}}(b) + 1$ by the shift $\frac{N+1}{4}$ while fixing the column sequences a and $L^{\frac{N+1}{2}}(a)$, we then get the sequence w in (13).

Theorem 7: The sequence w constructed by (13) is almost balanced, i.e.

$$N_0(w) = 2N - 1, \ N_1(w) = 2N + 1$$

or

$$N_0(w) = 2N + 1, \ N_1(w) = 2N - 1.$$

Theorem 8: w is a binary sequence of period $4N$ with optimal autocorrelation value, i.e., for $0 \leq \tau < 4N$

$$R_w(\tau) = \begin{cases} 4N, & 1 \text{ time} \\ 0, & 3N \text{ times} \\ -4, & N - 1 \text{ times.} \end{cases}$$

Proof: Writing $\tau = 4\tau_1 + \tau_2$, ($0 \leq \tau_1 < N$ and $0 < \tau_2 < 4$) or ($0 < \tau_1 < N$ and $\tau_2 = 0$), we consider the autocorrelation of w in four cases according to $\tau_2 = 0, 1, 2, 3$.

Case 1. $\tau_2 = 0$.

In this case, we have $0 < \tau_1 < N$, and then

$$\begin{aligned} R_w(\tau) &= R_a(\tau_1) + R_b(\tau_1) + R_a(\tau_1) + R_b(\tau_1) \\ &= -4. \end{aligned}$$

Case 2. $\tau_2 = 1$.

Applying (3) to the sequence w at $T = 4$ and $\tau_2 = 1$, we obtain

$$\begin{aligned} R_w(\tau) = & R_{a,b}\left(\tau_1 + \frac{N+1}{4}\right) \\ & + R_{b,a}\left(\tau_1 + \frac{N+1}{2} - \frac{N+1}{4}\right) \\ & - R_{a,b}\left(\tau_1 + \frac{3(N+1)}{4} - \frac{N+1}{2}\right) \\ & - R_{b,a}\left(\tau_1 + N + 1 - \frac{3(N+1)}{4}\right) \\ = & R_{a,b}\left(\tau_1 + \frac{N+1}{4}\right) + R_{b,a}\left(\tau_1 + \frac{N+1}{4}\right) \\ & - R_{a,b}\left(\tau_1 + \frac{N+1}{4}\right) - R_{b,a}\left(\tau_1 + \frac{N+1}{4}\right) \\ = & 0. \end{aligned}$$

Case 3. $\tau_2 = 2$.

By (3), we have

$$\begin{aligned}R_w(\tau) &= R_a\left(\tau_1 + \frac{N+1}{2}\right)\\ &\quad - R_b\left(\tau_1 + \frac{3(N+1)}{4} - \frac{N+1}{4}\right)\\ &\quad + R_a\left(\tau_1 + N + 1 - \frac{N+1}{2}\right)\\ &\quad - R_b\left(\tau_1 + \frac{N+1}{4} + N + 1 - \frac{3(N+1)}{4}\right)\\ &= R_a\left(\tau_1 + \frac{N+1}{2}\right) - R_b\left(\tau_1 + \frac{N+1}{2}\right)\\ &\quad + R_a\left(\tau_1 + \frac{N+1}{2}\right) - R_b\left(\tau_1 + \frac{N+1}{2}\right)\\ &= 0.\end{aligned}$$

Case 4. $\tau_2 = 3$.

Using similar arguments for Case 2, one can prove that $R_w(\tau) = 0$ for this case. ■

Remark 4: Construction B is a generalization of the ADS sequences proposed in [1]. In [17], an ADS sequence s was interpreted as

$$s = I\left(a, L^{\frac{N+1}{4}+\eta}(a), L^{\frac{N+1}{2}}(a), L^{\frac{3(N+1)}{4}+\eta}(a) + 1\right)$$

where $0 \leq \eta < N$ and $a = (a(t), t = 0, \ldots, N-1)$ is an ideal sequence of period N. Herein we get more sequences of period $4N$ with optimal autocorrelation value by changing the column sequences $L^{\frac{1}{4}+\eta}(a)$ and $L^{\frac{3}{4}+\eta}(a)+1$ as b and $L^{\frac{1}{2}}(b)+1$, where b is any ideal sequence of period N, which may be the same as the sequence a, or a shifted version of a, or a distinct one.

In addition, recall that in [16] a family of sequences of period $4N$ with optimal autocorrelation value has been constructed using (13) by setting $a = l$ and $b = l'$, where l and l' are, respectively, the first type and the second type of Legendre sequence of period N ($N = 3(\mathrm{mod}\ 4)$ odd prime).

In summary, Construction B is a generalization of all the constructions presented in the two papers [1], [16].

Example 3: Let a and b be two binary m-sequences of period 7 defined in Example 1. Then by Construction B, an almost balanced binary sequence of period 28 is generated as

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

It is easily calculated that v has optimal autocorrelation value

$$\begin{aligned}(R_w(\tau))_{\tau=0}^{27} = (&28,0,0,0,-4,0,0,0,-4,0,0,0,-4,0,0,\\ &0,-4,0,0,0,-4,0,0,0,-4,0,0,0).\end{aligned}$$

The following theorem characterizes the support of the binary sequence w, which is a direct consequence from the combinatorial characterization of the binary sequence with ideal autocorrelation given in Theorem 2.

Theorem 9: Let $\mathbf{W}$ be the support of the sequence w defined by (13). Then

$$\mathbf{W} = (\{0\} \times \mathbf{A}) \cup (\{1\} \times \mathbf{B}) \cup (\{2\} \times \mathbf{A}) \cup (\{3\} \times \mathbf{B})$$

is a $(4N, 2N+1, N, N-1)$ or $(4N, 2N-1, N-2, N-1)$ ADS over $\mathbf{Z}_4 \times \mathbf{Z}_N$, where $\mathbf{A}$ and $\mathbf{B}$ are, respectively, the $(N, (N+1)/2, (N+1)/4)$ or $(N, (N-1)/2, (N-3)/4)$ DS that are the supports of the ideal sequences a and b.

VII. Concluding Remarks and Open Problems

In this paper, we presented a construction of balanced quaternary sequences with period $N \equiv 2(\mathrm{mod}\ 4)$ and optimal autocorrelation value and a construction of almost balanced binary sequences of period $N \equiv 0(\mathrm{mod}\ 4)$ with optimal autocorrelation value. Both constructions are a generalization of earlier ones, and produce more sequences with optimal autocorrelation value.

Define

$$\begin{aligned}M_N = \min\{&\max_{0<\tau<N} |R_s(\tau)| : s\text{balanced quaternary}\\ &\text{sequence of period } N\}\end{aligned}$$

and

$$F_N = \min_{\substack{s\\ \max_{0<\tau<N} |R_s(\tau)| = M_N}} |\{0 < \tau < N : |R_s(\tau)| = M_N\}|$$

where s ranges over all balanced quaternary sequences S of period N with $|R_s(\tau)| = M_N$. Given that the cases of $N \equiv 0(\mathrm{mod}\ 4)$, $N \equiv 1(\mathrm{mod}\ 4)$, and $N \equiv 3(\mathrm{mod}\ 4)$ are still open, we propose the following problems.

Open Problem 1: For $N \equiv 1(\mathrm{mod}\ 4)$ and $N \equiv 3(\mathrm{mod}\ 4)$, determine the value M_N.

Open Problem 2: For $N \equiv 0(\mathrm{mod}\ 4)$, $N \equiv 1(\mathrm{mod}\ 4)$, and $N \equiv 3(\mathrm{mod}\ 4)$, determine the value F_N.

Once the two problems are solved, it would be interesting to construct balanced quaternary sequences of period N achieving the two minimum values M_N and F_N.

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. Inf. Theory*, vol. 47, no. 7, pp. 2934–2943, Nov. 2001.

[2] K. T. Arasu, W. D. Launey, and S. L. Ma, "On circulant Hadamard matrices," *Des., Codes and Crypt.*, vol. 25, no. 2, pp. 123–142, Feb. 2002.

[3] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," *IEEE Trans. Inf. Theory*, vol. 35, pp. 206–209, 1989.

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

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

[6] G. Gong, "New designs for signal sets with low cross correlation, balance property and large linear span: GF(p) case," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2847–2867, Nov. 2002.

[7] S. W. Golomb and G. Gong, *Signal Design for Good Correlation—For Wireless Communication, Cryptography and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[8] J.-W. Jang, Y.-S. Kim, S.-H. Kim, and J.-S. No, “New quaternary sequences with ideal autocorrelation constructed from binary sequences with ideal autocorrelation,” in *Proc. ISIT2009*, Seoul, Korea, Jun. 29–Jul. 3 2009, pp. 278–281.

[9] D. Jungnickel, , J. Dinitz and D. R. Stinson, Eds., *Contemporary Design Theory, A Collection of Surveys*, ser. Wiley-Interscience Series in Discrete Mathematics and Optimization. New York: Wiley, 1992, pp. 241–324.

[10] D. Jungnickel and B. Schmidt, , J. W. P. Hirschfeld, S. S. Magliveras, and M. J. de Resmini, Eds., *Geometry, Combinatorial Designs and Related Structures*. Cambridge, U.K.: Cambridge Univ. Press, 1997, pp. 89–112.

[11] Y.-S. Kim, J.-W. Jang, S.-H. Kim, and J.-S. No, “New construction of quaternary sequences with ideal autocorrelation from Legendre sequences,” in *Proc. ISIT2009*, Seoul, Korea, Jun. 29–Jul. 3 2009, pp. 282–285.

[12] Y.-S. Kim, J.-W. Jang, S.-H. Kim, and J.-S. No, “New quaternary sequences with optimal autocorrelation,” in *Proc. ISIT2009*, Seoul, Korea, Jun. 29–Jul. 3 2009, pp. 286–289.

[13] S. M. Krone and D. V. Sarwate, “Quadriphase sequences for spread spectrum multiple access communication,” *IEEE Trans. Inf. Theory*, vol. 30, no. 3, pp. 520–529, May 1984.

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

[15] P. Parraud, “On the non-existence of (almost-)perfect quaternary sequences,” in *Proc. AAECC-14*, S. Boztas and I. E. Shparlinski, Eds., 2001, vol. 2227, pp. 210–218, Lecture Notes in Comput. Sci., Springer Verlag.

[16] X. H. Tang and G. Gong, “New constructions of binary sequences with optimal autocorrelation value/magnitude,” *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1278–1286, Mar. 2010.

[17] N. Y. Yu and G. Gong, “New binary sequences with optimal autocorrelation magnitude,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4771–4779, Oct. 2008.

Xiaohu Tang (M’04) received the B.S. degree in applied mathematics from the Northwest Polytechnic University, Xi’an, China, the M.S. degree in applied mathematics from the Sichuan University, Chengdu, China, and the Ph.D. degree in electronic engineering from the Southwest Jiaotong University, Chengdu, China, in 1992, 1995, and 2001, respectively.

From 2003 to 2004, he was a postdoctoral researcher with the Department of Electrical and Electronic Engineering, Hong Kong University of Science and Technology. From 2007 to 2008, he was a visiting professor with University of Ulm, Germany. Since 2001, he has been with the Institute of Mobile Communications, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design, coding theory, and cryptography.

Dr. Tang was the recepient of the National excellent Doctoral Dissertation award in 2003 (China), the Humboldt Research Fellowship in 2007 (Germany).

Cunsheng Ding (M’98–SM’05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. degree in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992, he was Lecturer of Mathematics with Xidian University, China. He then joined the National University of Singapore, where he was Assistant Professor of Computer Science. He joined the Hong Kong University of Science and Technology in 2000, where he is currently Professor of Computer Science and Engineering. His research fields are cryptography and coding theory. He has coauthored four research monographs.

Dr. Ding was a corecipient of the State Natural Science Award of China in 1989. He served as a guest editor or editor for ten journals.