

# New Sets of Optimal Binary Low Correlation Zone Sequences

Ji-Woong JANG<sup>†</sup>, Jong-Seon NO<sup>†</sup>, Habong CHUNG<sup>††</sup>

<sup>†</sup> School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea.

<sup>††</sup> School of Electronics and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea.

E-mail: <sup>†</sup>{stseiya1,jsno}@snu.ac.kr, <sup>††</sup>habchung@hongik.ac.kr

**Abstract** In this paper, we propose new methods of constructing optimal binary low correlation zone(LCZ) sequences. In the new method, we devise a column sequence set of length  $2^{m+1} - 1$  from a binary sequence of period  $2^m - 1$  having ideal autocorrelation property and this column sequence set is used to construct binary LCZ sequence sets of period  $2^n - 1$  when  $(m+1)|n$ . The new method gives us the optimal sets with respect to the bound by Tang, Fan, and Matsufuji. Finally, we propose a construction method of  $2^n \times 2^n$  binary Hadamard matrices from optimal LCZ sequence sets.

**key words:** Binary sequence, Legendre sequence, low correlation zone(LCZ) sequence, sequence.

## 1. Introduction

Unlike the conventional code division multiple access(CDMA) systems, in the quasi-synchronous CDMA system[1] where maintaining synchronization within a few chips is feasible even in the reverse link due to the relatively small transmission delay, the most important property of the sequences used for reducing multiple access interference(MAI) is low correlation property around the origin[5]. Long, Zhang, and Hu[5] proposed the sequence set that has low correlation value around the origin, which can be used as a spreading sequence in the quasi-synchronous CDMA system. The sequence set with this property is called *low correlation zone(LCZ) sequence*. They also have shown that an LCZ sequence set has better performance than other well-known sequence sets with optimal correlation property[5]. For a prime  $p$ , Tang and Fan[9] proposed  $p$ -ary LCZ sequence sets by extending the alphabet size of each sequence in Long's work[5]. And they also proposed a construction method of  $p$ -ary LCZ sequence sets by using interleaved sequences[10]. Kim, Jang, No, and Chung proposed a new construction method of quaternary LCZ sequence sets by using binary sequence of the same period with ideal autocorrelation and they also calculated the correlation distributions of their sequence sets constructed from m-sequence and GMW sequence[3]. Their quaternary LCZ sequence set is optimal with respect to the bound by Tang, Fan, and Matsufuji[11]. But for a prime  $p$ , no optimal set of  $p$ -ary LCZ sequence set has been reported yet.

In this paper, we propose new methods of constructing optimal binary low correlation zone(LCZ) sequences. In the new method, we devise a column sequence set of length  $2^{m+1} - 1$  from a binary sequence of period  $2^m - 1$  having ideal autocorrelation property and this column sequence set is used to construct binary LCZ sequence sets of period  $2^n - 1$  when  $(m+1)|n$ . The new method gives us the optimal sets with respect to the bound by Tang, Fan, and

Matsufuji[11]. Finally, we propose a construction method of  $2^n \times 2^n$  binary Hadamard matrices from optimal LCZ sequence

## 2. Preliminaries

In this section, we introduce some definitions and notations.

Let  $\mathcal{S}$  be a set of  $D$  sequences of period  $N$ . If the magnitude of correlation function between any two sequences in  $\mathcal{S}$  takes the values less than or equal to  $\epsilon$  for the offset  $\tau$  in the range  $-Z < \tau < Z$ , then  $\mathcal{S}$  is called an  $(N, D, Z, \epsilon)$  LCZ sequence set.

Let  $p$  be a prime and  $F_{p^n}$  be the finite field with  $p^n$  elements. Let  $v_i(x)$  and  $v_j(x)$  be two  $p$ -ary sequences of period  $p^n - 1$ , defined in  $F_{p^n}^* = F_{p^n} \setminus \{0\}$ . Then for  $\delta \in F_{p^n}^*$ , the correlation function between two  $p$ -ary sequences  $v_i(x)$  and  $v_j(x)$  is defined as

$$R_{v_i, v_j}(\delta) = \sum_{x \in F_{p^n}^*} \omega_p^{v_i(x\delta) - v_j(x)}$$

where  $\omega_p$  is a complex primitive  $p$ -th root of unity. We will abuse the notation of the correlation function as  $R_{i,j}(\tau) = R_{v_i, v_j}(\alpha^\tau)$  for  $\delta = \alpha^\tau$ , where  $\alpha$  is a primitive element in  $F_{p^n}$ .

Let  $v(t)$  be a  $p$ -ary sequence of period  $p^n - 1$ . Then  $v(t)$  is said to have balance property if number of zero element is one less than that of each nonzero element in one period of the sequence. And if the sequence  $v(t) - v(t+\tau)$  is balanced for all  $\tau \not\equiv 0 \pmod{p^n - 1}$ , then  $v(t)$  is said to have difference-balance property.

The trace function  $\text{tr}_m^n(\cdot)$  from  $F_{p^n}$  to  $F_{p^m}$  is defined by

$$\text{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

where  $x \in F_{p^n}$  and  $m|n$ . The trace function has the following properties.

- (i)  $\text{tr}_m^n(ax+by) = a \text{tr}_m^n(x) + b \text{tr}_m^n(y)$ , for all  $a, b \in F_{p^m}$ ,  $x, y \in F_{p^n}$ .
- (ii)  $\text{tr}_m^n(x^{p^m}) = \text{tr}_m^n(x)$ , for all  $x \in F_{p^n}$ .

It is well known that  $\text{tr}_m^n(\alpha^t)$  is a  $p^m$ -ary m-sequence of period  $p^n - 1$ , where  $\alpha$  is a primitive element in  $F_{p^n}$ .

Klapper[4] introduced the  $d$ -form function. A  $d$ -form function  $H(x)$  on  $F_{p^n}$  over  $F_{p^m}$  is defined as a function satisfying for any  $y \in F_{p^m}$  and  $x \in F_{p^n}$

$$H(yx) = y^d H(x). \quad (1)$$

Kim, Jang, No, and Chung[3] derived the following lemma, which can be used in the proof of the subsequent theorem.

**Lemma 1** ([3]): Let  $m$  and  $n$  be positive integers such that  $m|n$ . Let  $A = \{1, \alpha, \dots, \alpha^{T-1}\}$ , where  $\alpha$  is a primitive element in  $F_{p^n}$  and  $T = (p^n - 1)/(p^m - 1)$ . Let  $h(x)$  be a 1-form function from  $F_{p^n}$  onto  $F_{p^m}$  with balance and difference-balance property. For a given  $\delta \in F_{p^n} \setminus F_{p^m}$ , let  $M_\delta(a, b)$  be the number of  $x_2 \in A$  satisfying

$$h(\delta x_2) = a \text{ and } h(x_2) = b, \quad a, b \in F_{p^m}. \quad (2)$$

Then, we have

$$\begin{aligned} M_\delta(0, 0) &= \frac{p^{n-2m} - 1}{p^m - 1} \\ \sum_{c \in F_{p^m}^*} M_\delta(c, 0) &= \sum_{c \in F_{p^m}^*} M_\delta(0, c) = p^{n-2m} \\ \sum_{d \in F_{p^m}^*} M_\delta(cd, d) &= p^{n-2m}, \text{ for any } c \in F_{p^m}^*. \end{aligned}$$

□

Tang and Fan[10] stated the following theorem using the interleaved sequence[2], which can be used for the construction of an LCZ sequence set.

**Theorem 2** ([10]): Let  $m$  and  $n$  be integers such that  $m|n$ . Let  $f(y)$  and  $g(y)$  be cyclically distinct sequences of period  $p^m - 1$  from  $F_{p^m}$  to  $F_p$  and the function  $h(x)$  from  $F_{p^n}$  to  $F_{p^m}$  be a 1-form function over  $F_{p^m}$  with balance and difference-balance property. If we set  $f(0) = g(0) = 0$ , then the correlation function  $R_{f,g}(\delta)$  between  $f(h(x))$  and  $g(h(x))$  is given as

$$\begin{aligned} R_{f,g}(\delta) &= \sum_{x \in F_{p^n}^*} \omega_p^{f(h(\delta x)) - g(h(x))} \\ &= \begin{cases} p^{n-m}(C_{f,g}(\delta) + 1) - 1, & \text{if } \delta \in F_{p^m} \\ p^{n-2m}(I(f) + 1)(\bar{I}(g) + 1) - 1, & \text{if } \delta \notin F_{p^m} \end{cases} \end{aligned}$$

where  $I(f) = \sum_{y \in F_{p^m}^*} \omega_p^{f(y)}$ ,  $C_{f,g}(\delta) = \sum_{y \in F_{p^m}^*} \omega_p^{f(\delta y) - g(y)}$ , and  $\bar{I}(\cdot)$  denotes complex conjugate of  $I(\cdot)$ . □

In the above theorem,  $f(\cdot)$  and  $g(\cdot)$  are called the *column sequences* of period  $p^m - 1$  in the two dimensional representation of the sequences  $f(h(\cdot))$  and  $g(h(\cdot))$  of period  $p^n - 1$ , respectively.

It is clear that  $I(f) = -1$  corresponds to the balance property of the column sequence  $f(y)$  defined on  $F_{p^m}^*$  if  $p$  is a prime. If the column sequences are balanced, we have

$$R_{f,g}(\delta) = -1, \text{ for } \delta \notin F_{p^m}.$$

In order to have  $R_{f,g}(1) = -1$ , we have to have  $C_{f,g}(1) = -1$ , which means that the in-phase cross-correlation function of each pair in the column sequence set has the value  $-1$ .

**Property 3:** Let  $\mathcal{A}$  be the set of sequences of period  $p^m - 1$  satisfying the following properties:

- i) All the sequences in the set  $\mathcal{A}$  are cyclically distinct.
- ii) Each sequence in the set  $\mathcal{A}$  has the balance property.
- iii) In-phase cross-correlation value of each pair of the sequences in the set  $\mathcal{A}$  is always  $-1$ .

□

Theorem 2 tells us that if we have the sequence set  $\mathcal{A}$  satisfying Property 3, then the  $(p^n - 1, |\mathcal{A}|, (p^n - 1)/(p^m - 1), 1)$   $p$ -ary LCZ sequence set can be constructed.

In the subsequent sections, we propose methods of constructing the column sequence sets satisfying Property 3, some of which are of the maximum size.

### 3. New optimal binary LCZ sequence sets

In this section, for integers  $n$  and  $m$  such that  $(m + 1)|n$ , we construct the optimal binary LCZ sequence set of period  $2^n - 1$  by using binary sequences of period  $2^m - 1$  with ideal autocorrelation.

The following lemma can be easily stated without proof.

**Lemma 4:** Let  $m_1(t)$  and  $m_2(t)$  be two cyclically distinct  $p$ -ary sequences with linear span  $L_1$  and  $L_2$ , respectively. The maximum run lengths of the symbol 0 and the symbol  $a$ ,  $1 \leq a \leq p - 1$ , for the difference sequence  $m_1(t) - m_2(t)$  are less than or equal to  $L_1 + L_2 - 1$  and  $L_1 + L_2$ , respectively. □

Using two binary sequences with ideal autocorrelation, we can construct a set of column sequences satisfying Property 3 as in the following theorem.

**Theorem 5:** : Let  $m_1(t)$  and  $m_2(t)$  be two binary sequences, not necessarily distinct, of period  $2^m - 1$  with ideal autocorrelation. Let  $L_1$  and  $L_2$  be the linear spans of the sequences  $m_1(t)$  and  $m_2(t)$ , respectively, such that  $L_1 + L_2 + \max(L_1, L_2) < 2^m - 1$  and in addition,  $L_1 = L_2 < 2^{m-1}$ , if  $m_1$  and  $m_2$  are cyclically equivalent. Define the new sequences  $s_i(t)$ ,  $0 \leq i \leq 2^{m+1} - 2$  of period  $2^{m+1} - 1$  such that

- i) for  $0 \leq i \leq 2^m - 2$

$$s_i(t) = \begin{cases} m_1(t + i), & 0 \leq t \leq 2^m - 2 \\ 0, & t = 2^m - 1 \\ m_2(t - 1 - i), & 2^m \leq t \leq 2^{m+1} - 2 \end{cases} \quad (3)$$

- ii) for  $2^m - 1 \leq i \leq 2^{m+1} - 3$

$$s_i(t) = \begin{cases} m_1(t + i), & 0 \leq t \leq 2^m - 2 \\ 1, & t = 2^m - 1 \\ m_2(t - 1 - i) + 1, & 2^m \leq t \leq 2^{m+1} - 2 \end{cases} \quad (4)$$

and

$$s_{2^{m+1}-2}(t) = \begin{cases} 0, & 0 \leq t \leq 2^m - 2 \\ 1, & 2^m - 1 \leq t \leq 2^{m+1} - 2. \end{cases}$$

Then the set of sequences  $s_i(t)$  satisfies Property 3.

*Proof:* From the definition of  $s_i(t)$ , it is clear that  $s_i(t)$  is balanced and it is also easy to see that the in-phase cross-correlation  $C_{s_i, s_j}(1)$  between  $s_i(t)$  and  $s_j(t)$  takes the value  $-1$ .

Certainly the last sequence  $s_{2^{m+1}-2}(t)$  is cyclically

distinct to every other sequence. What we are going to show is that for any  $i, j, 0 \leq i, j \leq 2^{m+1} - 3$ , and  $\tau$ ,  $s_j(t) = s_i(t + \tau)$  implies that  $i = j$  and  $\tau = 0$ .

**Case 1)**  $0 \leq i, j \leq 2^m - 3$  and  $0 \leq \tau \leq 2^m - 2$

It is not difficult to see that  $s_i(t + \tau)$  can be expressed as:

$$s_i(t + \tau) = \begin{cases} m_1(t + i + \tau), & 0 \leq t \leq 2^m - 2 - \tau \\ 0, & t = 2^m - 1 - \tau \\ m_2(t - 1 - i + \tau), & 2^m - \tau \leq t \leq 2^{m+1} - 2 - \tau \\ m_1(t + i + \tau - 1), & 2^{m+1} - 1 - \tau \leq t \leq 2^{m+1} - 2. \end{cases} \quad (5)$$

Assume  $s_j(t) = s_i(t + \tau)$  for all  $t$ . From (3) and (5), we have

$$m_1(t + j) + m_1(t + i + \tau) = 0, \quad 0 \leq t \leq 2^m - 2 - \tau \quad (6)$$

$$m_1(t + j) + m_2(t - 1 - i + \tau) = 0, \quad 2^m - \tau \leq t \leq 2^m - 2 \quad (7)$$

$$m_2(t - 1 - j) + m_2(t - 1 - i + \tau) = 0, \quad 2^m \leq t \leq 2^{m+1} - 2 - \tau \quad (8)$$

$$m_2(t - 1 - j) + m_1(t + i + \tau - 1) = 0, \quad 2^{m+1} - 1 - \tau \leq t \leq 2^{m+1} - 2. \quad (9)$$

Equations (6) and (8) tell us that

$$m_1(t + j) = m_1(t + i + \tau)$$

and

$$m_2(t - 1 - j) = m_2(t - 1 - i + \tau)$$

for consecutive  $2^m - 1 - \tau$  values of  $t$ . Thus if  $\tau < 2^m - \max(L_1, L_2)$ , i.e.,  $2^m - 1 - \tau \geq \max(L_1, L_2)$ , then we have  $j = i - \tau = i + \tau$ , which further tells us that  $i = j$  and  $\tau = 0$ . Note that in this case (7) and (9) become meaningless. If  $\tau \geq 2^m - \max(L_1, L_2)$ , then (7) and (9) tell us that

$$m_1(t + j) = m_2(t - 1 - i + \tau)$$

and

$$m_2(t - 1 - j) = m_1(t + i + \tau - 1)$$

for consecutive  $\tau - 1$  and  $\tau$  values of  $t$ , respectively, which is impossible from Lemma 4 unless  $m_1(t)$  and  $m_2(t)$  are cyclically equivalent, since  $\tau - 1 \geq L_1 + L_2$ . Thus, satisfying (7) and (9) at the same time means that  $m_1(t)$  and  $m_2(t)$  are cyclically equivalent and  $i + j = \tau - 1 = -\tau$ , which further implies  $\tau = 2^{m-1}$ . But  $\tau = 2^{m-1}$  is not in the range  $\tau \geq 2^m - \max(L_1, L_2)$ , since  $\max(L_1, L_2) < 2^{m-1}$ .

**Case 2)**  $0 \leq i, j \leq 2^m - 3$  and  $2^m \leq \tau \leq 2^{m+1} - 2$

In this case,  $s_i(t + \tau)$  can be expressed as:

$$s_i(t + \tau) = \begin{cases} m_2(t - 1 - i + \tau), & 0 \leq t \leq 2^{m+1} - 2 - \tau \\ 0, & t = 2^m - 1 - \tau \\ m_1(t + i + \tau), & 2^{m+1} - 1 - \tau \leq t \leq 2^{m+1} + 2^m - 3 - \tau \\ m_2(t - 2 - i + \tau), & 2^{m+1} + 2^m - 1 - \tau \leq t \leq 2^{m+1} - 2. \end{cases} \quad (10)$$

Assume  $s_j(t) = s_i(t + \tau)$  for all  $t$ . From (3) and (10), we have

$$m_1(t + j) + m_2(t - 1 - i + \tau) = 0, \quad 0 \leq t \leq 2^{m+1} - 2 - \tau$$

$$m_1(t + j) + m_1(t + i + \tau) = 0, \quad 2^{m+1} - 1 - \tau \leq t \leq 2^m - 2$$

$$m_2(t - 1 - j) + m_1(t + i + \tau) = 0, \quad 2^m \leq t \leq 2^{m+1} + 2^m - 3 - \tau$$

$$m_2(t - 1 - j) + m_2(t - 2 - i + \tau) = 0, \quad 2^{m+1} + 2^m - 1 - \tau \leq t \leq 2^{m+1} - 2.$$

Similarly to Case 1), we can deduce that  $s_j(t) = s_i(t + \tau)$  implies  $i = j$  and  $\tau = 0$ .

**Case 3)**  $2^m - 1 \leq i, j \leq 2^{m+1} - 3$  and  $0 \leq \tau \leq 2^m - 2$

In this case,  $s_i(t + \tau)$  can be expressed as:

$$s_i(t + \tau) = \begin{cases} m_1(t + i + \tau), & 0 \leq t \leq 2^m - 2 - \tau \\ 1, & t = 2^m - 1 - \tau \\ m_2(t - 1 - i + \tau) + 1, & 2^m - \tau \leq t \leq 2^{m+1} - 2 - \tau \\ m_1(t + i + \tau - 1), & 2^{m+1} - 1 - \tau \leq t \leq 2^{m+1} - 2. \end{cases} \quad (11)$$

Assume  $s_j(t) = s_i(t + \tau)$  for all  $t$ . From (4) and (11), we have

$$m_1(t + j) + m_1(t + i + \tau) = 0, \quad 0 \leq t \leq 2^m - 2 - \tau \quad (12)$$

$$m_1(t + j) + m_2(t - 1 - i + \tau) = 1, \quad 2^m - \tau \leq t \leq 2^m - 2 \quad (13)$$

$$m_2(t - 1 - j) + m_2(t - 1 - i + \tau) = 0, \quad 2^m \leq t \leq 2^{m+1} - 2 - \tau \quad (14)$$

$$m_2(t - 1 - j) + m_1(t + i + \tau - 1) = 1, \quad 2^{m+1} - 1 - \tau \leq t \leq 2^{m+1} - 2. \quad (15)$$

Using the similar argument in Case 1), we can derive contradiction for some of (12)–(15) from Lemma 4.

**Case 4)**  $2^m - 1 \leq i, j \leq 2^{m+1} - 3$  and  $2^m \leq \tau \leq 2^{m+1} - 2$

In this case,  $s_i(t + \tau)$  can be expressed as:

$$s_i(t+\tau) = \begin{cases} m_2(t-1-i+\tau)+1, & 0 \leq t \leq 2^{m+1}-2-\tau \\ 0, & t = 2^m-1-\tau \\ m_1(t+i+\tau), & \\ 2^{m+1}-1-\tau \leq t \leq 2^{m+1}+2^m-3-\tau \\ m_2(t-2-i+\tau)+1, & \\ 2^{m+1}+2^m-1-\tau \leq t \leq 2^{m+1}-2. \end{cases} \quad (16)$$

Assume  $s_j(t) = s_i(t+\tau)$  for all  $t$ . From (4) and (16), we have

$$m_1(t+j) + m_2(t-1-j+\tau) = 1, \quad 0 \leq t \leq 2^{m+1}-2-\tau \quad (17)$$

$$m_1(t+j) + m_1(t+i+\tau) = 0, \quad 2^{m+1}-1-\tau \leq t \leq 2^m-2 \quad (18)$$

$$m_2(t-1-j) + m_1(t+i+\tau) = 1, \quad 2^m \leq t \leq 2^{m+1}+2^m-3-\tau \quad (19)$$

$$m_2(t-1-j) + m_2(t-2-j+\tau) = 0, \quad 2^{m+1}+2^m-1-\tau \leq t \leq 2^{m+1}-2. \quad (20)$$

Using the similar argument in Case 1), we can derive contradiction for some of (17)–(20) using Lemma 4.

**Case 5)**  $2^m-1 \leq i \leq 2^{m+1}-3$ ,  $0 \leq j \leq 2^m-2$ , and  $0 \leq \tau \leq 2^m-2$

In this case,  $2^m-1 \leq i \leq 2^{m+1}-3$ ,  $s_i(t+\tau)$  can be expressed as:

$$s_i(t+\tau) = \begin{cases} m_1(t+i+\tau), & 0 \leq t \leq 2^m-2-\tau \\ 1, & t = 2^m-1-\tau \\ m_2(t-1-i+\tau)+1, & \\ 2^m-\tau \leq t \leq 2^{m+1}-2-\tau \\ m_1(t+i+\tau-1), & \\ 2^{m+1}-1-\tau \leq t \leq 2^{m+1}-2. \end{cases} \quad (21)$$

Assume  $s_j(t) = s_i(t+\tau)$  for all  $t$ . From (3) and (21), we have

$$m_1(t+j) + m_1(t+i+\tau) = 0, \quad 0 \leq t \leq 2^m-2-\tau \quad (22)$$

$$m_1(t+j) + m_2(t-1-i+\tau) = 1, \quad 2^m-\tau \leq t \leq 2^m-2 \quad (23)$$

$$m_2(t-1-j) + m_2(t-1-i+\tau) = 1, \quad 2^m \leq t \leq 2^{m+1}-2-\tau \quad (24)$$

$$m_2(t-1-j) + m_1(t+i+\tau-1) = 0, \quad 2^{m+1}-1-\tau \leq t \leq 2^{m+1}-2. \quad (25)$$

Similarly to Case 1), we can also derive contradiction for some of (22)–(25) using Lemma 4.

**Case 6)**  $2^m-1 \leq i \leq 2^{m+1}-3$ ,  $0 \leq j \leq 2^m-2$ , and  $2^m \leq \tau \leq 2^{m+1}-2$

In this case,  $s_i(t+\tau)$  can be expressed as:

$$s_i(t+\tau) = \begin{cases} m_2(t-1-i+\tau)+1, & 0 \leq t \leq 2^{m+1}-2-\tau \\ 0, & t = 2^m-1-\tau \\ m_1(t+i+\tau), & \\ 2^{m+1}-1-\tau \leq t \leq 2^{m+1}+2^m-3-\tau \\ m_2(t-2-i+\tau)+1, & \\ 2^{m+1}+2^m-1-\tau \leq t \leq 2^{m+1}-2. \end{cases} \quad (26)$$

Assume  $s_j(t) = s_i(t+\tau)$  for all  $t$ . From (3) and (26), we have

$$m_1(t+j) + m_2(t-1-i+\tau) = 1, \quad 0 \leq t \leq 2^{m+1}-2-\tau \quad (27)$$

$$m_1(t+j) + m_1(t+i+\tau) = 0, \quad 2^{m+1}-1-\tau \leq t \leq 2^m-2 \quad (28)$$

$$m_2(t-1-j) + m_1(t+i+\tau) = 0, \quad 2^m \leq t \leq 2^{m+1}+2^m-3-\tau \quad (29)$$

$$m_2(t-1-j) + m_2(t-2-i+\tau) = 1, \quad 2^{m+1}+2^m-1-\tau \leq t \leq 2^{m+1}-2. \quad (30)$$

Using the similar argument in Case 1), we derive contradiction for some of (27)–(30) using Lemma 4.

**Case 7)**  $\tau = 2^m-1$

In this case, it is straightforward that  $s_i(t+\tau) \neq s_j(t)$ ,  $0 \leq i, j \leq 2^{m+1}-3$ .

From the above 7 cases, we proved that  $s_i(t)$  and  $s_j(t)$  are cyclically distinct for all  $i$  and  $j$ . Thus, we proved that the set of sequences  $s_i(t)$  satisfies Property 3.  $\square$

Note that the conditions for linear spans of  $m_1(t)$  and  $m_2(t)$  in Theorem 5 are sufficient not necessary. Even though we cannot directly apply Theorem 5 to the Legendre sequence with  $m_1(t) = m_2(t)$ , whose linear span is half of the period, we can see that all  $s_i(t)$  constructed from Legendre sequence are also cyclically distinct because the run lengths of 1 in the difference sequence of Legendre sequence and its cyclic shift cannot exceed  $2^{m-1}-1$ .

Using Theorem 2 and the column sequence sets in Theorem 5, we can construct the binary LCZ sequence sets as in the following theorem.

**Theorem 6:** Let  $n$  and  $m$  be integers such that  $(m+1)|n$  and  $T = (2^n-1)/(2^{m+1}-1)$ . Let  $\alpha$  be a primitive element in  $F_{2^n}$  and  $\beta = \alpha^T$  be a primitive element in  $F_{2^{m+1}}$ . Let  $h(x)$  from  $F_{2^n}$  to  $F_{2^{m+1}}$  be a 1-form function over  $F_{2^{m+1}}$  with balance and difference-balance property, i.e., either a  $2^{m+1}$ -ary m-sequence, a  $2^{m+1}$ -ary GMW sequence, or a  $2^{m+1}$ -ary generalized GMW sequence. Let  $f_i(\beta^t) = s_i(t)$ , where  $s_i(t)$  is the binary sequence defined in Theorem 5. Then the sequence set  $\mathcal{B}$  defined by

$$\mathcal{B} = \{v_i(t) = f_i(h(\alpha^t)) \mid 0 \leq i \leq 2^{m+1}-2, 0 \leq t \leq 2^n-2\}$$

is a binary LCZ sequence set with parameters  $(2^n-1, 2^{m+1}-1, T, 1)$ .  $\square$

Tang, Fan, and Matsufuji[11] derived the lower bound on LCZ sequences using the Welch bound[12].

**Theorem 7** (Tang, Fan, and Matsufuji[11]): Let  $\mathcal{S}$  be a set of LCZ sequences with parameters  $(N, D, Z, \epsilon)$ . Then,

$$DZ - 1 \leq \frac{N - 1}{1 - \epsilon^2/N}. \quad (31)$$

□

Now we can check the optimality of our binary LCZ sequence set  $\mathcal{B}$ .

**Corollary 8:** The binary LCZ sequence set  $\mathcal{B}$  in Theorem 6 is optimal with respect to the Tang-Fan-Matsufuji bound given in Theorem 7.

*Proof:* The proof is straightforward. By substituting  $N = 2^n - 1$ ,  $D = 2^{m+1} - 1$ , and  $\epsilon = 1$  in (31), we have

$$(2^{m+1} - 1)Z - 1 \leq \frac{2^n - 2}{1 - 1/(2^n - 1)}$$

and thus

$$Z \leq \frac{2^n}{2^{m+1} - 1}.$$

Since  $Z$  is an integer, we have

$$Z \leq \left\lfloor \frac{2^n}{2^{m+1} - 1} \right\rfloor = \frac{2^n - 1}{2^{m+1} - 1} = T.$$

Clearly,  $\mathcal{B}$  is optimal with respect to the Tang-Fan-Matsufuji bound. □

## Acknowledgments

This work was supported by Lab. of Excellency program and ITRC program

## References

- [1] R. De Gaudenzi, C. Elia, and R. Viola, "Bandlimited quasisynchronous CDMA: A novel satellite access technique for mobile and personal communication system," *IEEE J. Select. Area Commun.*, vol. 10, pp. 328-343, Feb. 1992.
- [2] G. Gong, "Theory and applications of  $q$ -ary interleaved sequences," *IEEE Trans. Inform. Theory*, vol. 41, pp. 400-411, Mar. 1995.
- [3] S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1469-1477, April 2005.
- [4] A. Klapper, " $d$ -form sequence: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423-431, Mar. 1995.
- [5] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Technol.*, vo. 47, pp. 1268-1275, Nov. 1998.
- [6] Jong-Seon No, " $p$ -ary unified sequences:  $p$ -ary extended  $d$ -form sequences with ideal autocorrelation property," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2540-2546, September 2002.
- [7] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. on Inform. Theory*, vol. 42, no. 6, pp. 2254-2255, Nov. 1996.
- [8] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proc. IEEE Int. Symp. Inform. Theory and Its Appl. (ISITA'96)*, Victoria, British Columbia, Canada, Sept. 1996, pp. 837-840.
- [9] X. H. Tang and P. Z. Fan, "A class of pseudonoise sequences over  $GF(p)$  with low correlation zone," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1644-1649, May 2001.
- [10] X. H. Tang and P. Z. Fan, "Large families of generalized  $d$ -form sequences with low correlations and large linear span based on the interleaved technique," preprint, 2004.
- [11] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlatoin zone," *Electon. Lett.*, vol. 36, no. 6, pp. 551-552, Mar. 2000.
- [12] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, no. 3, pp. 397-399, May 1974.