

# New Sets of Optimal $p$ -ary Low Correlation Zone Sequences

Ji-Woong Jang  
Channel Development Team  
System LSI Division  
Samsung Electronics Co.  
Suwon 443-742, Korea.  
Email: roy.jang@samsung.com

Jung-Soo Chung, Jong-Seon No  
School of EE and CS  
Seoul National University  
Seoul 151-742, Korea.  
Email: jsno@snu.ac.kr

Habong Chung  
School of Electronics and Electrical Engineering  
Hongik University  
Seoul 121-791, Korea  
Email: habchung@hongik.ac.kr

**Abstract**—In this paper, we propose the new construction methods of constructing optimal low correlation zone(LCZ) sequences. We construct the new  $p$ -ary LCZ sequence sets by adopting  $p$ -ary sequence of period  $p^m - 1$  with ideal autocorrelation for integers  $n$  and  $m$  such that  $m|n$  as a column sequence. The new construction methods give us the optimal sets with respect to the bound by Tang, Fan, and Matsufuji.

## I. 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[6]. Long, Zhang, and Hu[6] 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[6]. For a prime  $p$ , Tang and Fan[8] proposed  $p$ -ary LCZ sequence sets by extending the alphabet size of each sequence in Long's work[6]. And they also proposed a construction method of  $p$ -ary LCZ sequence sets by using interleaved sequences[9]. 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[4]. Their quaternary LCZ sequence set is optimal with respect to the bound by Tang, Fan, and Matsufuji[10]. But for a prime  $p$ , no optimal set of  $p$ -ary LCZ sequence set has been reported yet.

In this paper, we propose new construction methods of constructing optimal LCZ sequences. We construct the new  $p$ -ary LCZ sequence sets by adopting  $p$ -ary sequence of period  $p^m - 1$  with ideal autocorrelation for integers  $n$  and  $m$  such that  $m|n$  as a column sequence. The new construction methods

give us the optimal sets with respect to the bound by Tang, Fan, and Matsufuji[10].

## II. 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[5] 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[4] derived the following lemma, which can be used in the proof of the subsequent theorem.

**Lemma 1 (Kim, Jang, No, and Chung[4]):** 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

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

Then, we have

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

□

Tang and Fan[9] stated the following theorem using the interleaved sequence[2], which can be used for the construction of an LCZ sequence set.

**Theorem 2 (Tang and Fan[9]):** 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

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

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  $I(\cdot)$ .

*Proof:* Since Theorem 2 is slightly modified from its original version in [9], we will give the alternate proof.

**Case 1**  $\delta \in F_{p^m}$

Since  $h(x)$  is a 1-form function,  $h(\delta x) = \delta h(x)$ . Let  $N_h(a)$  be the number of  $x \in F_{p^n}^*$  such that  $h(x) = a$ . Then we can

rewrite  $R_{f,g}(\delta)$  as follows

$$\begin{aligned} R_{f,g}(\delta) &= \sum_{x \in F_{p^n}^*} \omega_p^{f(h(\delta x)) - g(h(x))} \\ &= \sum_{x \in F_{p^n}^*} \omega_p^{f(\delta h(x)) - g(h(x))} \\ &= \sum_{y \in F_{p^m}} N_h(y) \omega_p^{f(\delta y) - g(y)}. \end{aligned}$$

From the balance property of  $h(x)$ ,  $N_h(y)$  has the following values

$$N_h(y) = \begin{cases} p^{n-m} - 1, & \text{if } y = 0 \\ p^{n-m}, & \text{otherwise.} \end{cases}$$

Therefore, when  $\delta \in F_{p^m}$ ,  $R_{f,g}(\delta)$  is given as

$$R_{f,g}(\delta) = p^{n-2m} C_{f,g}(\delta) + p^{n-2m} - 1.$$

**Case 2**  $\delta \notin F_{p^m}$

Let  $T = (p^n - 1)/(p^m - 1)$ . Let  $x = x_1 x_2$ , where  $x_1 \in F_{p^m}$  and  $x_2 \in A = \{1, \alpha, \alpha^2, \dots, \alpha^{T-1}\}$ . For  $\delta \notin F_{p^m}$ , with the replacement of  $h(\delta x_2)$  by  $cd$  and  $h(x_2)$  by  $d$  and also from Lemma 1,  $R_{f,g}(\delta)$  is rewritten as

$$\begin{aligned} R_{f,g}(\delta) &= \sum_{x \in F_{p^n}^*} \omega_p^{f(h(\delta x)) - g(h(x))} \\ &= \sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd, d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 cd) - g(x_1 d)} \\ &\quad + M_\delta(0, 0) \sum_{x_1 \in F_{p^m}^*} \omega_p^0 \\ &\quad + \sum_{c \in F_{p^m}^*} M_\delta(c, 0) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 c)} \\ &\quad + \sum_{c \in F_{p^m}^*} M_\delta(0, c) \sum_{x_1 \in F_{p^m}^*} \omega_p^{-g(x_1 c)} \\ &= \sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd, d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 cd) - g(x_1 d)} \\ &\quad + p^{n-2m} - 1 + p^{n-2m} I(f) + p^{n-2m} \bar{I}(g). \quad (3) \end{aligned}$$

The first term in the right-hand side of (3) can be rewritten as

$$\begin{aligned} &\sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd, d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 cd) - g(x_1 d)} \\ &= \sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd, d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 c) - g(x_1)} \\ &= p^{n-2m} \sum_{c \in F_{p^m}^*} \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 c) - g(x_1)}. \quad (4) \end{aligned}$$

Since  $f(\cdot)$  and  $g(\cdot)$  are cyclically distinct, (4) can be rewritten as

$$p^{n-2m} \left( \sum_{x_1 \in F_{p^m}^*} \omega_p^{-g(x_1)} \right) \left( \sum_{c \in F_{p^m}^*} \omega_p^{f(c)} \right) = p^{n-2m} I(f) \bar{I}(g).$$

Therefore, we have

$$R_{f,g}(\delta) = p^{n-2m}(1 + I(f))(1 + \bar{I}(g)) - 1. \quad \square$$

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

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

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.

### III. NEW OPTIMAL $p$ -ARY LCZ SEQUENCE SETS

In this section, for a prime  $p$  and integers  $n$  and  $m$  such that  $m|n$ , we propose a new construction method of the optimal  $p$ -ary LCZ sequence set of period  $p^n - 1$  by using a  $p$ -ary sequence of period  $p^m - 1$  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.

□

Jang, No, and Chung proposed a construction method of column sequence set constructed by similar method in this paper for optimal binary LCZ sequence set[3].

*Theorem 5 (Jang, No, and Chung[3]):* 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  $0 \leq i \leq 2^m - 2$

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

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

$$s_i(t) = \begin{cases} m_1(t+i), & 0 \leq t \leq 2^m - 2 \\ 1, & t = 2^m - 1 \\ m_2(t-1-i) + 1, & 2^m \leq t \leq 2^{m+1} - 2 \end{cases} \quad (6)$$

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. □

They also proposed an optimal binary LCZ sequence set using Theorem 2 and the column sequence set in the above theorem[3].

*Theorem 6 (Jang, No and Chung[3]):* 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  $(2^n - 1, 2^{m+1} - 1, T, 1)$ . □

In the next theorem, we construct a set of  $p$ -ary cyclically distinct sequences of period  $p^m - 1$  satisfying Property 3 from a  $p$ -ary sequence with ideal autocorrelation.

*Theorem 7:* Let  $p$  be a prime and  $m(t)$  be a  $p$ -ary sequence with ideal autocorrelation of period  $M = p^m - 1$ . Let  $L_m$  be the linear span of  $m(t)$  and  $\{m_i(t) \mid 0 \leq i \leq M - 1\}$  be a set of cyclic shifts of  $m(t)$ , such that  $m_i(t) = m(t+i)$ ,  $t = 0, 1, 2, \dots, M - 1$ . Define new sequences  $s_i(t)$ ,  $0 \leq i \leq M - 1$ , such that

$$s_i(t) = \begin{cases} m_i(M-1-t), & 0 \leq t \leq M-K-1 \\ m_i(t+K), & M-K \leq t \leq M-1 \end{cases} \quad (7)$$

for some integer  $K$  in the range  $3L_m - 1 \leq K \leq M/2$ . Then the set of  $p$ -ary sequences  $s_i(t)$ ,  $0 \leq i \leq M - 1$  satisfies Property 3.

*Proof:* From the definition of  $s_i(t)$ , it is clear that all  $s_i(t)$  are 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  $-1$ .

Now, what we have to show is that for any  $i, j$ , and  $\tau$ ,  $s_j(t) = s_i(t + \tau)$  implies that  $i = j$  and  $\tau = 0$ . The sequence  $s_i(t)$  in (7) can be rewritten as

$$s_i(t) = \begin{cases} m(M-1-t+i), & 0 \leq t \leq M-K-1 \\ m(t+i+K), & M-K \leq t \leq M-1. \end{cases} \quad (8)$$

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

**Case 1)**  $0 \leq \tau \leq M-K-1$

$$s_i(t + \tau) = \begin{cases} m(M-1-t-\tau+i), & 0 \leq t \leq M-K-1-\tau \\ m(t+\tau+i+K), & M-K-\tau \leq t \leq M-\tau-1 \\ m(M-1-t-\tau+i), & M-\tau \leq t \leq M-1. \end{cases} \quad (9)$$

Assume  $s_j(t) = s_i(t + \tau)$  for all  $t$ . Then from (8) and (9), we have

$$m(M-1-t+j) = m(M-1-t-\tau+i), \quad 0 \leq t \leq M-K-1-\tau \quad (10)$$

$$m(M-1-t+j) = m(t+\tau+i+K), \quad M-K-\tau \leq t \leq M-K-1 \quad (11)$$

$$m(t+j+K) = m(t+\tau+i+K), \quad M-K \leq t \leq M-\tau-1 \quad (12)$$

$$m(t+j+K) = m(M-1-t-\tau+i), \quad M-\tau \leq t \leq M-1. \quad (13)$$

Here, we consider the following two cases depending on  $\tau$ .

When  $\tau \leq 2L_m - 1$ , both  $(M-K-\tau)$  and  $(K-\tau)$  are greater than or equal to  $L_m$  since  $3L_m - 1 \leq K \leq M/2$ . From (10), we have

$$m(M-1-t+j) - m(M-1-t-\tau+i) = 0 \quad (14)$$

for consecutive  $M-K-\tau$  values of  $t$ . And similarly from (12), we have

$$m(t+j+K) - m(t+\tau+i+K) = 0 \quad (15)$$

for consecutive  $K-\tau$  values of  $t$ . It is clear that the linear span of  $m(t) - m(t+k)$  for all  $k$ ,  $1 \leq k \leq p^m - 2$ , is  $L_m$ . Since both  $M-K-\tau$  and  $K-\tau$  are greater than or equal to  $L_m$ , (14) and (15) imply that

$$j = i - \tau = i + \tau$$

which further tells us that  $i = j$  and  $\tau = 0$ . And again in this case, (11) and (13) vanish.

When  $\tau \geq 2L_m$ , (11) or (13) implies that some consecutive  $\tau$  bits of two sequences  $m(t)$  and  $m(-t)$  are identical, which is a contradiction from Lemma 4 since the linear span of  $m(t) - m(-t+k)$  for all  $k$ ,  $0 \leq k \leq p^m - 2$ , is at most  $2L_m$ .

**Case 2)**  $\tau \geq M - T$

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

$$s_i(t + \tau) = \begin{cases} m(t+K+i+\tau), & 0 \leq t \leq M-1-\tau \\ m(M-t+i-1-\tau), & M-\tau \leq t \leq 2M-K-\tau-1 \\ m(t+K+i+\tau), & 2M-\tau-K \leq t \leq M-1. \end{cases}$$

Again, assuming  $s_j(t) = s_i(t + \tau)$  gives us

$$m(M-1-t+j) = m(t+K+i+\tau), \quad 0 \leq t \leq M-1-\tau \quad (16)$$

$$m(M-1-t+j) = m(M-t+i-1-\tau), \quad M-\tau \leq t \leq M-K-1 \quad (17)$$

$$m(t+j+K) = m(M-t+i-1-\tau), \quad M-K \leq t \leq 2M-K-\tau-1 \quad (18)$$

$$m(t+j+K) = m(t+T+i+\tau), \quad 2M-K-\tau \leq t \leq M-1. \quad (19)$$

When  $\tau \geq (M-K) + L_m$ , both  $\tau - K$  and  $\tau - (M-K)$  are greater than or equal to  $L_m$ , since  $M-K > K$ . From (17), we have

$$m(M-1-t+j) - m(M-t+i-1-\tau) = 0$$

for consecutive  $(\tau - K)$  values of  $t$ . And from (19), we have

$$m(t+j+K) - m(t+K+i+\tau) = 0$$

for consecutive  $\tau - (M-K)$  values of  $t$ . Similarly to Case 1), since both  $\tau - K$  and  $\tau - (M-K)$  are greater than or equal to  $L_m$ , we can deduce  $i = j$  and  $\tau = 0$ .

When  $\tau \leq (M-K) + L_m - 1$ , we have  $M - \tau \geq 2L_m$ . Therefore, either (16) or (18) implies that some consecutive  $M - \tau$  bits of two cyclically inequivalent sequences are identical, which is again a contradiction from Lemma 4.  $\square$

Note that even if we limit the range of  $K$  as  $3L_m - 1 \leq K \leq M/2$  in Theorem 7 for the sake of the simplicity of the proof, in fact the theorem holds for all  $K$  such that  $3L_m - 1 \leq K \leq M - (3L_m - 1)$ . If  $3L_m - 1 > M/2$ , the above theorem cannot be directly applied. But there are many sequences with  $3L_m - 1 > M/2$ , the set of which obtained as in Theorem 7 satisfies Property 3. For example, the sequences  $s_i(t)$  in (7) constructed from the binary m-sequence with  $L_m = 4$  of period  $M = 15$  are all cyclically distinct for  $K = 7$ . The proof for such cases should be further investigated into.

Using Theorem 2 and the column sequence set in Theorem 7, we can construct the  $p$ -ary LCZ sequence sets as in the following theorem.

**Theorem 8:** Let  $p$  be a prime and  $n$  and  $m$  be integers such that  $m|n$ . Let  $T = (p^n - 1)/(p^m - 1)$  and  $M = p^m - 1$ . Let  $\alpha$  be a primitive element in  $F_{p^n}$  and  $\beta = \alpha^T$  be a primitive element in  $F_{p^m}$ . Let  $h(x)$  from  $F_{p^n}$  to  $F_{p^m}$  be a 1-form function over  $F_{p^m}$  with balance and difference-balance property, i.e., a  $p^m$ -ary unified sequence[7] which includes an m-sequence, a GMW sequence, and a generalized GMW

sequence. Let  $f_i(\beta^t) = s_i(t)$ , where  $s_i(t)$  is the sequence defined in Theorem 7. Then the following sequence set  $\mathcal{P}$  defined by

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

is a LCZ sequence set with parameters  $(p^n - 1, p^m - 1, T, 1)$ .  $\square$

Tang, Fan, and Matsufuji[10] derived the lower bound on LCZ sequences using the Welch bound[11].

*Theorem 9 (Tang, Fan, and Matsufuji[10]):* Let  $\mathcal{S}$  be a set of LCZ sequences with parameters  $(N, D, Z, \epsilon)$ . Then,

$$DZ - 1 \leq \frac{N - 1}{1 - \epsilon^2/N}. \quad (20)$$

$\square$

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

*Corollary 10:* The  $p$ -ary LCZ sequence set  $\mathcal{P}$  in Theorem 8 is optimal with respect to the Tang-Fan-Matsufuji bound given in Theorem 9.

*Proof :* The proof is straightforward. By substituting  $N = p^n - 1$ ,  $D = p^m - 1$ , and  $\epsilon = 1$  in (20), we have

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

and thus

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

Since  $Z$  is an integer, we have

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

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

#### ACKNOWLEDGEMENT

This work was supported by University IT Research Center Project and Laboratory of Excellency 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] Ji-Woong Jang, Jong-Seon No, and Habong Chung, "New sets of optimal binary low correlation zone sequences," *Proc. The second International Workshop on Sequence Design and its Application in Comm.*(Shimonoseki, Yamaguchi, Japan), October 10-14, 2005, pp. 73-77.
- [4] S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *IEEE Trans. on Inform. Theory*, vol. 51, no. 4, pp. 1469-1477, April 2005.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlatoin zone," *Electron. Lett.*, vol. 36, no. 6, pp. 551-552, Mar. 2000.
- [11] 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.