New Low Correlation Zone Sequence Sets With Flexible LCZ and Set Size [1]

*Young-Sik Kim^{O}, *Ji-Woong Jang, *Jong-Seon No, and **Habong Chung
*School of Electrical Engineering and Computer Science and INMC, Seoul National University
**School of Electronics and Electrical Engineering, Hong-Ik University
Email: jsno@snu.ac.kr

Abstract

In this paper, we propose a design scheme for LCZ sequence sets with parameters $(2^{n+1}-2, M, L, 2)$. In this scheme, we can freely choose the LCZ length L and the resulting LCZ sequence set has the size M, which is nearly optimal with respect to Tang, Fan, and Matsufuji bound.

1. Introduction

Let S be a set of M sequences of period N. If the magnitudes of correlation function between any two sequences in S take the values less than or equal to ϵ within the range, $-L < \tau < L$, of the offset τ, then S is called an (N, M, L, ϵ) LCZ sequence set. Long, Zhang, and Hu [4] proposed a binary LCZ sequence set by using Gordon-Mills-Welch (GMW) sequences. Kim, Jang, No, and Chung [3] proposed optimal quaternary LCZ sequence sets. And Jang, No, Chung, and Tang [2] constructed new optimal p-ary LCZ sequence sets.

Ding, Helleseth, and Martinsen [1] proposed the new families of binary sequences with optimal three-level autocorrelation using cyclotomic number of order 4. Utilizing the interleaving technique in their work, we propose a new design scheme for LCZ sequence sets with parameters $(2^{n+1}-2, M, L, 2)$. In this scheme, we can freely set the LCZ length L and the resulting LCZ sequence set has the size M, which is nearly optimal with respect to Tang, Fan, and Matsufuji bound.

2. Design of New Sequence Sets

Let $N = 2^{n+1}-2$. Let Z_N be the set of integers modulo N, i.e., $Z_N = \{0, 1, \cdots, N-1\}$. Let $a(t)$ be a binary sequence of period $2^n - 1$ with ideal autocorrelation.

Let D_u be the characteristic set of $a(t-u)$, i.e.,

$$D_u = \{t \mid a(t-u) = 1, 0 \le t \le 2^n - 2\} = D_0 + u$$

where $u \in Z_{2^n-1}$, $D_0 + u = \{d + u \mid d \in D_0\}$, and "+" means addition modulo $2^n - 1$. Let $\overline{D}_u = Z_{2^n-1} \backslash D_u$. From the balancedness of $a(t)$, we have

$$|D_u| = 2^{n-1} \quad (1)$$
$$|\overline{D}_u| = 2^{n-1} - 1. \quad (2)$$

From the difference-balance property of $a(t)$, for $u \ne v$, we have

$$|D_u \cap D_v| = 2^{n-2} \quad (3)$$
$$|D_u \cap \overline{D}_v| = 2^{n-2} \quad (4)$$
$$|\overline{D}_u \cap \overline{D}_v| = 2^{n-2} - 1. \quad (5)$$

By the Chinese remainder theorem, we have $Z_N \cong Z_2 \otimes Z_{2^n-1}$ under the isomorphism $\phi : w \mapsto (w \bmod 2, w \bmod 2^n - 1)$. Throughout the paper, we use the notations $w \in Z_N$ and $(w \bmod 2, w \bmod 2^n - 1)$, interchangeably.

For $u \in Z_{2^n-1}$, let C_u be the subset of Z_N such that

$$C_u \cong \{0\} \otimes A_u \cup \{1\} \otimes D_{1-u} \quad (6)$$

where A_u can be either D_u or $\overline{D}_u$. Then we have

$$|C_u| = \begin{cases} |D_u| + |D_{1-u}| = 2^n, & \text{if } A_u = D_u \\ |\overline{D}_u| + |D_{1-u}| = 2^n - 1, & \text{if } A_u = \overline{D}_u. \end{cases} \quad (7)$$

Let $s_u(t)$ be the characteristic sequence of C_u. Note that just like C_u which can be one of two distinct subsets of Z_N depending on A_u, the sequence $s_u(t)$ can also take one of two distinct sequences, one with 2^n 1's and the other with $2^n - 1$ 1's. The correlation function $R_{u,v}(\tau)$ of binary sequences $s_u(t)$ and $s_v(t)$ of period N is defined as

$$R_{u,v}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_u(t)+s_v(t+\tau)}.$$

Let $d_{u,v}(\tau) = |C_u \cap (C_v + \tau)|$, where $\tau \in Z_N$, $C_v + \tau = \{c + \tau \mid c \in C_v\}$, and "+" means the addition modulo N. Then we can easily check the following lemma.

Lemma 1 The correlation function $R_{u,v}(\tau)$ can be expressed as

$$R_{u,v}(\tau) = N - 2(|C_u| + |C_v| - 2d_{u,v}(\tau)).$$

□

[1] This research was supported by the MIC, Korea, under the ITRC support program and by the MOE, the MOCIE, and the MOLAB, Korea, through the fostering project of the Lab. of Excellency.

Now let us define two sets of characteristic sequences of C_u in (6).

Definition 2 The set $\mathcal{U}_1$ is the collection of all the characteristic sequences $s_u(t)$, $1 \leq u < 2^{n-1}$, of C_u with $A_u = D_u$. Similarly, the collection of all the characteristic sequences $s_u(t)$, $1 \leq u < 2^{n-1}$, of C_u with $A_u = \overline{D}_u$ is called the set $\mathcal{U}_2$. □

The following theorem gives us the correlation values of the sequences in Definition 2.

Theorem 3 The correlation functions of two sequences $s_u(t)$ and $s_v(t)$ in $\mathcal{U}_1 \cup \mathcal{U}_2$ are as follows:
Case 1) $s_u(t)$, $s_v(t) \in \mathcal{U}_1$;
i) $u \neq v$;

$$R_{u,v}(\tau) = \begin{cases} 2^n - 2, & \text{for } \tau = (0, u-v), (0, v-u), \\ & \quad (1, u+v-1), (1, 1-u-v) \\ -2, & \text{otherwise.} \end{cases}$$

ii) $u = v$;

$$R_{u,u}(\tau) = \begin{cases} 2^{n+1} - 2, & \text{for } \tau = 0 \\ 2^n - 2, & \text{for } \tau = (1, 2u-1), (1, 1-2u) \\ -2, & \text{otherwise.} \end{cases}$$

Case 2) $s_u(t) \in \mathcal{U}_1$ and $s_v(t) \in \mathcal{U}_2$;
i) $u \neq v$;

$$R_{u,v}(\tau) = \begin{cases} -2^n, & \text{for } \tau = (0, u-v), (1, 1-u-v) \\ 2^n, & \text{for } \tau = (0, v-u), (1, u+v-1) \\ 0, & \text{otherwise.} \end{cases}$$

ii) $u = v$;

$$R_{u,u}(\tau) = \begin{cases} -2^n, & \text{for } \tau = (1, 1-2u) \\ 2^n, & \text{for } \tau = (1, 2u-1) \\ 0, & \text{otherwise.} \end{cases}$$

Case 3) $s_u(t)$, $s_v(t) \in \mathcal{U}_2$;
i) $u \neq v$;

$$R_{u,v}(\tau) = \begin{cases} 2^n - 2, & \text{for } \tau = (0, u-v), (0, v-u) \\ -2^n + 2, & \text{for } \tau = (1, u+v-1), (1, 1-u-v) \\ -2, & \text{for } \tau = (0, \tau_2), \tau_2 \neq \pm(u-v) \\ 2, & \text{for } \tau = (1, \tau_2), \tau_2 \neq \pm(u+v-1). \end{cases}$$

ii) $u = v$;

$$R_{u,u}(\tau) = \begin{cases} 2^{n+1} - 2, & \text{for } \tau = 0 \\ -2^n + 2, & \text{for } \tau = (1, 2u-1), (1, 1-2u) \\ -2, & \text{for } \tau = (0, \tau_2), \tau_2 \neq 0 \\ 2, & \text{for } \tau = (1, \tau_2), \tau_2 \neq \pm(2u-1). \end{cases}$$

Proof: Let $\tau = (\tau_1, \tau_2) \in Z_2 \otimes Z_{2^n-1}$. From Definition 2, it is clear that $u + v \not\equiv 1 \bmod 2^n - 1$. Then we have

$$\begin{aligned} d_{u,v}(\tau) &= |C_u \cap (C_v + \tau)| \\ &= |\{0\} \cap \{\tau_1\}||A_u \cap (A_v + \tau_2)| \\ &\quad + |\{0\} \cap \{1 + \tau_1\}||A_u \cap (D_{1-v} + \tau_2)| \\ &\quad + |\{1\} \cap \{\tau_1\}||D_{1-u} \cap (A_v + \tau_2)| \\ &\quad + |\{1\} \cap \{1 + \tau_1\}||D_{1-u} \cap (D_{1-v} + \tau_2)| \\ &= \begin{cases} |A_u \cap (A_v + \tau_2)| + |D_{1-u} \cap (D_{1-v} + \tau_2)|, \\ \qquad \text{for } \tau_1 = 0 \\ |A_u \cap (D_{1-v} + \tau_2)| + |D_{1-u} \cap (A_v + \tau_2)|, \\ \qquad \text{for } \tau_1 = 1. \end{cases} \end{aligned} \tag{8}$$

Case 1) $s_u(t)$, $s_v(t) \in \mathcal{U}_1$;
In this case, we have $A_u = D_u$ and $A_v = D_v$.
i) $u \neq v$;
From (8), we have

$$d_{u,v}(\tau) = \begin{cases} |D_u| + |D_{1-u} \cap D_{u-2v+1}|, & \text{for } \tau = (0, u-v) \\ |D_u \cap D_{2v-u}| + |D_{1-u}|, & \text{for } \tau = (0, v-u) \\ |D_u \cap (D_v + \tau_2)| + |D_{1-u} \cap (D_{1-v} + \tau_2)|, \\ \qquad \text{for } \tau = (0, \tau_2), \tau_2 \neq \pm(u-v) \\ |D_u| + |D_{1-u} \cap D_{u+2v-1}|, & \text{for } \tau = (1, u+v-1) \\ |D_u \cap D_{2-u-2v}| + |D_{1-u}|, & \text{for } \tau = (1, 1-u-v) \\ |D_u \cap (D_{1-v} + \tau_2)| + |D_{1-u} \cap (D_v + \tau_2)|, \\ \qquad \text{for } \tau = (1, \tau_2), \tau_2 \neq \pm(u+v-1). \end{cases} \tag{9}$$

Applying (1) and (3) in (9), we have

$$d_{u,v}(\tau) = \begin{cases} 2^{n-1} + 2^{n-2}, & \text{for } \tau = (0, u-v), (0, v-u), \\ & \quad (1, u+v-1), (1, 1-u-v) \\ 2^{n-1}, & \text{otherwise.} \end{cases}$$

From Lemma 1 and (7), we have

$$R_{u,v}(\tau) = \begin{cases} 2^n - 2, & \text{for } \tau = (0, u-v), (0, v-u), \\ & \quad (1, u+v-1), (1, 1-u-v) \\ -2, & \text{otherwise.} \end{cases}$$

ii) $u = v$;
This case corresponds to autocorrelation of the sequences in $\mathcal{U}_1$ and we have

$$\begin{aligned} d_{u,u}(\tau) &= \begin{cases} |D_u \cap |D_u + \tau_2| + |D_{1-u} \cap (D_{1-u} + \tau_2)|, \\ \qquad \text{for } \tau_1 = 0 \\ |D_u \cap |D_{1-u} + \tau_2| + |D_{1-u} \cap (D_u + \tau_2)|, \\ \qquad \text{for } \tau_1 = 1 \end{cases} \\ &= \begin{cases} 2^n, & \text{for } \tau = 0 \\ 2^{n-1} + 2^{n-2}, & \text{for } \tau = (1, 2u-1), (1, 1-2u) \\ 2^{n-1}, & \text{otherwise.} \end{cases} \end{aligned}$$

Then we have

$$R_{u,u}(\tau) = \begin{cases} 2^{n+1}-2, & \text{for } \tau=0 \\ 2^n-2, & \text{for } \tau=(1,2u-1),(1,1-2u) \\ -2, & \text{otherwise.} \end{cases} \quad (10)$$

Case 2) $s_u(t) \in \mathcal{U}_1$ and $s_v(t) \in \mathcal{U}_2$;

In this case, we have $A_u = D_u$ and $A_v = \overline{D}_v$.

i) $u \neq v$;

From (8), we have

$$d_{u,v}(\tau) = \begin{cases} |D_u \cap \overline{D}_u| + |D_{1-u} \cap D_{u-2v+1}|, & \text{for } \tau=(0,u-v) \\ |D_u \cap \overline{D}_{2v-u}| + |D_{1-u}|, & \text{for } \tau=(0,v-u) \\ |D_u \cap (\overline{D}_v+\tau_2)| + |D_{1-u} \cap (D_{1-v}+\tau_2)|, & \\ & \text{for } \tau=(0,\tau_2), \tau_2 \neq \pm(u-v) \\ |D_u| + |D_{1-u} \cap \overline{D}_{u+2v-1}|, & \text{for } \tau=(1,u+v-1) \\ |D_u \cap D_{2-u-2v}| + |D_{1-u} \cap \overline{D}_{1-u}|, & \\ & \text{for } \tau=(1,1-u-v) \\ |D_u \cap (D_{1-v}+\tau_2)| + |D_{1-u} \cap (\overline{D}_v+\tau_2)|, & \\ & \text{for } \tau=(1,\tau_2), \tau_2 \neq \pm(u+v-1). \end{cases}$$

Applying (1)–(4), we have

$$d_{u,v}(\tau) = \begin{cases} 2^{n-2}+0, & \text{for } \tau=(0,u-v),(1,1-u-v) \\ 2^{n-2}+2^{n-1}, & \text{for } \tau=(0,v-u),(1,u+v-1) \\ 2^{n-1}, & \text{otherwise} \end{cases}$$

which yields

$$R_{u,v}(\tau) = \begin{cases} -2^n, & \text{for } \tau=(0,u-v),(1,1-u-v) \\ 2^n, & \text{for } \tau=(0,v-u),(1,u+v-1) \\ 0, & \text{otherwise.} \end{cases}$$

ii) $u = v$;

We have

$$R_{u,u}(\tau) = \begin{cases} -2^n, & \text{for } \tau=(1,1-2u) \\ 2^n, & \text{for } \tau=(1,2u-1) \\ 0, & \text{otherwise.} \end{cases}$$

Case 3) $s_u(t)$, $s_v(t) \in \mathcal{U}_2$;

In this case, we have $A_u = \overline{D}_u$ and $A_v = \overline{D}_v$.

i) $u \neq v$;

Similarly, applying (1)–(5) and $|D_u \cap \overline{D}_u| = 0$ in (8), we have

$$R_{u,v}(\tau) = \begin{cases} 2^n-2, & \text{for } \tau=(0,u-v),(0,v-u) \\ -2^n+2, & \text{for } \tau=(1,u+v-1),(1,1-u-v) \\ -2, & \text{for } \tau=(0,\tau_2), \tau_2 \neq \pm(u-v) \\ 2, & \text{for } \tau=(1,\tau_2), \tau_2 \neq \pm(u+v-1). \end{cases}$$

ii) $u = v$;

Similarly to (10), autocorrelation function of the sequences in $\mathcal{U}_2$ can be obtained as

$$R_{u,u}(\tau) = \begin{cases} 2^{n+1}-2, & \text{for } \tau=0 \\ -2^n+2, & \text{for } \tau=(1,2u-1),(1,1-2u) \\ -2, & \text{for } \tau=(0,\tau_2), \tau_2 \neq 0 \\ 2, & \text{for } \tau=(1,\tau_2), \tau_2 \neq \pm(2u-1). \end{cases}$$

□

Note that Case 1)-ii) and Case 3)-ii) correspond to autocorrelation functions. Also note that there are two sidelobes, i.e., correlation magnitude exceeding two, for each correlation function with $u = v$, and four sidelobes, otherwise. In the next section, we design LCZ sequence sets by selecting appropriate sequences in $\mathcal{U}_1 \cup \mathcal{U}_2$.

3. Constructions of Nearly Optimal LCZ Sequence Sets

In this section, we will propose two methods of selecting sequences in $\mathcal{U}_1 \cup \mathcal{U}_2$, so that the set consisting of the selected sequences forms an LCZ sequence set which is nearly optimal with respect to the following bound.

Theorem 4 [Tang, Fan, and Matsufuji [5]] Let $\mathcal{S}$ be an LCZ sequence set with parameters (N, M, L, ϵ). Then we have

$$ML - 1 \leq \frac{N-1}{1-\epsilon^2/N}. \quad (11)$$

□

For $\epsilon = 2$, $n \geq 4$, (11) becomes

$$M \leq \left\lfloor \frac{N+4}{L} \right\rfloor \quad (12)$$

where $\lfloor x \rfloor$ means the greatest integer less than or equal to x. When an $(N, M, L, 2)$ LCZ set achieves the equality in (12), it is said to be optimal.

Recall that the locations of sidelobes are symmetric with respect to the origin. Thus, in terms of the distances to the sidelobes from the origin, there are at most two distinct distances. Let $L_{u,v}$ denote the distance to the nearest sidelobes from the origin in $R_{u,v}(\tau)$. Then, $L_{u,v}$ can be determined as in the following lemma, which is not difficult to prove.

Lemma 5 For $s_u(t), s_v(t) \in \mathcal{U}_1 \cup \mathcal{U}_2$, $1 \leq v \leq u < 2^{n-1}$, $L_{u,v}$ is given as

$$L_{u,v} = \begin{cases} \frac{N}{2}-u-v+1, & \text{if } u-v \text{ is odd} \\ u-v, & \text{if } u-v \text{ is even and } u \neq v \\ 2u-1, & \text{if } u=v. \end{cases} \quad (13)$$

□

Lemma 5 tells us that the LCZ of a set of sequences $s_u(t)$'s chosen from $\mathcal{U}_1 \cup \mathcal{U}_2$ is solely dependent on the index values u's regardless of whether the sequence $s_u(t)$ is from $\mathcal{U}_1$ or $\mathcal{U}_2$.

Thus what we are going to do now is to choose an index set $I \subset \{1, 2, \cdots, 2^{n-1}-1\}$ and construct the set of sequences

$$W_I = \{s_u(t) \in \mathcal{U}_1 \mid u \in I\} \cup \{s_u(t) \in \mathcal{U}_2 \mid u \in I\}$$

so that W_I becomes a good LCZ sequence set.

Lemma 5 tells us that the LCZ of the set W_I is the minimum of the following three values: $2^n-(u+v)$ for odd $|u-v|$, $|u-v|$ for nonzero even $|u-v|$, and $2u-1$ for $u=v$ as u and v run over I.

Thus, to maintain a given parameter L, the LCZ of the set W_I, the indices in I should be greater than or equal to $(L+1)/2$, sum of two indices should be less than or equal to 2^n-L unless their differences are even, and their differences should not be even numbers less than L. At the same time, for a given L, we want to make the size of I as large as possible.

From these constraints, we can formulate fairly complex optimal design problem. The solution for this problem seems somewhat complicated, but aforementioned constraints implicitly lead us to consider an index set I which forms an arithmetic progression with odd value of common difference.

Construction 1: Pick an odd integer f and a nonnegative integer $f_0 \le 1$. Then we make an index set I as

$$I=\left\{f_0+mf \;\middle|\; m=1,2,\cdots,\left\lfloor\frac{2^{n-1}-f_0}{f}\right\rfloor\right\}.$$

□

Then it is not difficult to show that the set size M and LCZ L of W_I in Construction 1 are given as in the following theorem.

Theorem 6 Let q and r be the quotient and the remainder of 2^{n-1}, respectively, when divided by f, i.e., $2^{n-1}=qf+r$. Then W_I from Construction 1 becomes a binary LCZ sequence set with parameters $(2^{n+1}-2, M, L, 2)$, where M and L are given as

$$M=2q \tag{14}$$

$$L=\begin{cases} f+2r-2f_0, & \text{for } f\ge 2r+1-3f_0\\ 2f-1+f_0, & \text{for } f<2r+1-3f_0.\end{cases} \tag{15}$$

□

In the following construction method, we allow two distinct values $f+2$ and f for the difference values between adjacent indices.

Construction 2: The indices u of the selected sequences $s_u(t)$ both in $\mathcal{U}_1$ and in $\mathcal{U}_2$ are chosen to form a progression starting from $f+2-f_0$ with differences f and $f+2$, alternately, i.e.,

$$I=\{u_j \mid j=0,1,2,\cdots,J,\ u_0=f+2-f_0,\ u_{2k+1}-u_{2k}=f,\ u_{2k+2}-u_{2k+1}=f+2\}$$

where J is the largest integer such that $u_J<2^{n-1}$, f_0 is 0 or 1, and f is some odd integer. □

The set size M and LCZ L are given as the following theorem.

Theorem 7 Let q and r be the quotient and the remainder of $2^{n-1}-1$, respectively, when divided by $2(f+1)$, i.e., $2^{n-1}-1=2q(f+1)+r$. Then W_I from Construction 2 becomes a binary LCZ sequence set with parameters $(2^{n+1}-2, M, L, 2)$, where M and L are given as

$$M=\begin{cases} 4q, & \text{for } 0\le r<f+2-f_0\\ 4q+2, & \text{for } f+2-f_0\le r<2f+2\end{cases}$$

$$L=\begin{cases} 2r+f+2+2f_0, & \text{for } 0\le r<\frac{f-3f_0}{2}\\ 2f+2-f_0, & \text{for } \frac{f-3f_0}{2}\le r<f+2-f_0\\ & \quad\text{and } \frac{3f+2-3f_0}{2}\le r<2f+2\\ 2r-f+2f_0, & \text{for } f+2-f_0\le r<\frac{3f+2-3f_0}{2}.\end{cases} \tag{16}$$

Proof: From Lemma 5 and the fact that f is odd, L is the smallest value of $2f+2$, $2(f+2-f_0)-1$, and $2^n-(u+v)$ where u and v are the largest and the second largest elements in I.

If $0\le r<f+2-f_0$, then $|I|=2q$ and $u+v=4q(f+1)-f-2f_0$. Thus, $2^n-(u+v)=f+2+2r+2f_0$. Therefore we have

$$L=\min\{2f+2, 2f+3-2f_0, f+2+2r+2f_0\}. \tag{17}$$

If $f+2-f_0\le r<2f+2$, then $|I|=2q+1$ and $u+v=4q(f+1)+f+2-2f_0$. Thus $2^n-(u+v)=2r-f+2f_0$. Therefore we have

$$L=\min\{2f+2, 2f+3-2f_0, 2r-f+2f_0\}. \tag{18}$$

We can obtain (16) from (17) and (18). □

References

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

[2] J.-W. Jang, J.-S. No, H. Chung, and X. Tang, "New sets of optimal p-ary low correlation zone sequences," submitted to *IEEE Trans. Inf. Theory*, Mar. 2005.

[3] S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, Apr. 2005.

[4] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Technol.*, vol. 47, no. 6, pp. 1268–1275, Nov. 1998.

[5] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlation zone," *Electron. Lett.*, vol. 36, no. 6, pp. 551–552, Mar. 2000.