# Quaternary LCZ Sequences Constructed From m-Sequences [1]

*Sang-Hyo Kim, *Ji-Woong Jang O, *Jong-Seon No, and +Habong Chung
*Seoul National University, +Hongik University
{kimsh,stasera}@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

Abstract

In this paper, given a composite integer $n$, we propose a method of constructing quaternary low correlation zone(LCZ) sequences of period $2^n-1$ from binary m-sequences of the same length. The correlation distribution of these new quaternary LCZ sequences is derived.

## I. Introduction

In a microcellular communication environment such as wireless LAN where the cell size is very small, transmission delay is relatively small and thus it is possible to maintain the time delay in reverse link within a few chip. In such a system as the quasi-synchronous code-division multiple-access(QS-CDMA) system proposed by Gaudenzi, Elia, and Vilola[1], multiple chip time delay among different users are allowed, which gives more flexibility in designing the wireless communication system.

In the design of sequences for QS-CDMA system, what matters most is to have low correlation zone around orgin rather than to minimize maximum nontrivial correlation value[5]. In fact, low correlation zone(LCZ) sequences show better performance than other well-known sequence sets with optimal correlation property. Let $\mathcal{S}$ be a set of $M$ 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 $\epsilon$ within the range $-L < \tau < L$, of the offset $\tau$, then $\mathcal{S}$ is called an $(N, M, L, \epsilon)$ LCZ sequence set.

In this paper, given a composite integer $n$, we propose a method of constructing quaternary low correlation zone(LCZ) sequences of period $2^n-1$ from binary m-sequences of the same length. The correlation distribution of these new quaternary LCZ sequences is derived.

## II. Preliminaries

In this section, we introduce some definitions and notations.

Let $F_{2^n}$ be the finite field with $2^n$ elements. The trace function $\mathrm{tr}_m^n(\cdot)$ from $F_{2^n}$ to $F_{2^m}$ is defined by $\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{mi}}$, where $x \in F_{2^n}$ and $m|n$. It is well known that $\mathrm{tr}_1^n(\alpha^t)$ is a binary m-sequence of period $2^n-1$, where $\alpha$ is a primitive element in $F_{2^n}$.

In this paper, we only deal with binary and quaternary sequences of period $2^n-1$, which can be regarded as mappings from $F_{2^n}$ to $F_2$ and to an integer ring $Z_4 = \{0,1,2,3\}$, respectively. We use the notations $\boxplus$ for the addition in $Z_4$, only if we think it is necessary.

Let $F_{2^n}^* = F_{2^n} \setminus \{0\}$ and $s(x)$ be a mapping from $F_{2^n}$ to $F_2$ or $Z_4$. When we restrict the mapping $s(x)$ to $F_{2^n}^*$ and replace $x$ by $\alpha^t$, then we can obtain a sequence $s(\alpha^t)$, $0 \le t \le 2^n-2$, of period $2^n-1$. Hence, for convenience, we will use the expression 'a binary or quaternary sequence $s(\alpha^t)$ of period $2^n-1$' interchangeably with 'a mapping $s(x)$ from $F_{2^n}$ to $F_2$ or $Z_4$'.

For $\delta \in F_{2^n}^*$, the crosscorrelation function between two quaternary sequences $s_i(x)$ and $s_j(x)$ is defined as

$$R_{i,j}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{s_i(x\delta) - s_j(x)}$$

where $w_4$ is a complex fourth root of unity.

It is not difficult to see that a quaternary sequences can be decomposed into two constituent binary sequences. Let $v_1$ and $v_2$ be variables over $Z_2$, i.e., Boolean variables. Then a variable $v$ over $Z_4$ can be expressed as

$$v = v_1 \boxplus 2v_2. \tag{1}$$

Let us use the notation $v = (v_2, v_1)$ to alternatively represent (1). Let $\phi(\cdot)$ and $\psi(\cdot)$ be the maps defined by

$$\phi(v) = v_1, \quad \psi(v) = v_2.$$

Using the expression $(v_2, v_1)$, we can obtain the truth tables for $\phi(v-w)$ and $\psi(v-w)$ given in Table 1.

Let $v(x)$, $w(x)$, and $d(x)$ be quaternary sequences given as

$$v(x) = v_1(x) \boxplus 2v_2(x), \quad w(x) = w_1(x) \boxplus 2w_2(x)$$

[1] This work was supported in part by BK21 and ITRC program.

Table 1: Truth tables for $\phi(v-w)$ and $\psi(v-w)$.

| $\phi(v-w)$ | $w$ =(0,0) | (0,1) | (1,1) | (1,0) |
|---|---|---|---|---|
| $v$ =(0,0) | 0 | 1 | 1 | 0 |
| (0,1) | 1 | 0 | 0 | 1 |
| (1,1) | 1 | 0 | 0 | 1 |
| (1,0) | 0 | 1 | 1 | 0 |

| $\psi(v-w)$ | $w$ =(0,0) | (0,1) | (1,1) | (1,0) |
|---|---|---|---|---|
| $v$ =(0,0) | 0 | 1 | 0 | 1 |
| (0,1) | 0 | 0 | 1 | 1 |
| (1,1) | 1 | 1 | 0 | 0 |
| (1,0) | 1 | 0 | 1 | 0 |

and

$$d(x) = v(x) - w(x)$$

where $x \in F_{2^n}^*$. Using Karnaugh map and Table 1, the mappings $\phi$ and $\psi$ of the quaternary sequence $d(x)$ are given by

$$\begin{aligned} \phi(d(x)) &= v_1(x) + w_1(x) && (2) \\ \psi(d(x)) &= v_1(x)w_1(x) + w_1(x) + w_2(x) + v_2(x). && (3) \end{aligned}$$

## III. Construction of Quaternary LCZ Sequences

In this section, we construct a set of quaternary LCZ sequence using an m-sequences as their constituent sequences. The following lemma is useful in the computation of correlation of these quaternary LCZ sequences.

**Lemma 1** : Let $s(x)$ be a function from $F_{2^n}$ to $Z_4$, where $s(0) = 0$. We define two Boolean constituent functions of $s(x)$ as

$$\phi_s(x) = \phi(s(x)), \quad \psi_s(x) = \psi(s(x))$$

and their modulo-2 sum as

$$\mu_s(x) = \phi_s(x) + \psi_s(x).$$

Let $N_f(c)$ denote the number of occurrences of $f(x) = c$ as $x$ varies over $F_{2^n}$. Then, we have

$$\sum_{x \in F_{2^n}} \omega_4^{s(x)} = (N_{\psi_s}(0) - N_{\mu_s}(1)) + j(N_{\mu_s}(1) - N_{\psi_s}(1)). \quad (4)$$

*Proof :* It is clear that

$$\sum_{x \in F_{2^n}} \omega_4^{s(x)} = (N_s(0) - N_s(2)) + j(N_s(1) - N_s(3)). \quad (5)$$

Equation (4) can be easily obtained from the followings :

$$\begin{aligned} N_{\psi_s}(1) &= N_s(2) + N_s(3) && (6) \\ N_{\psi_s}(0) &= 2^n - N_{\psi_s}(1) = N_s(0) + N_s(1) && (7) \\ N_{\mu_s}(1) &= N_s(1) + N_s(2). && (8) \end{aligned}$$

□

From above lemma, it is clear that the function $s(x)$ is balanced if and only if $\psi_s(x)$ and $\mu_s(x)$ are balanced.

Let $f(x)$ be a function from $F_{2^n}$ to $F_2$. We can use $f(x)$ as the constituent sequence of a quaternary sequence $q(x)$ as

$$q(x) = f(x) \boxplus 2f(ax)$$

where $a \in F_{2^n} \backslash F_2$. We can derive the crosscorrelation values between two quaternary sequences constructed from an m-sequence.

**Theorem 1** : Let $m_a(x)$ and $m_b(x)$ be two quaternary sequences defined by the functions

$$\begin{aligned} m_a(x) &= \mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(ax) \\ m_b(x) &= \mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(bx) \end{aligned}$$

where $a, b \in F_{2^n} \backslash F_2$. Then, their crosscorrelation values are given as

$$R_{a,b}(\delta) = \begin{cases} 2^n - 1, & a = b \text{ and } \delta = 1 \\ -1 + 2^{n-1}, & a \neq b \text{ and } \delta = \frac{b}{a} \text{ or } \frac{b+1}{a+1} \\ -1 + j2^{n-1}, & \delta = \frac{b+1}{a} \\ -1 - j2^{n-1}, & \delta = \frac{b}{a+1} \\ -1, & \text{otherwise} \end{cases}$$

where $j = \sqrt{-1}$.

*Proof :* Let $d(x) = m_a(\delta x) - m_b(x)$. The crosscorrelation function between two sequences $m_a(x)$ and $m_b(x)$ is given by

$$R_{a,b}(\delta) = \sum_{x \in F_{2^n}^*} w_4^{d(x)} = -1 + \sum_{x \in F_{2^n}} w_4^{d(x)}. \quad (9)$$

From (2) and (3), we have

$$\begin{aligned} \phi_d(x) &= \mathrm{tr}_1^n(\delta x) + \mathrm{tr}_1^n(x) \\ \psi_d(x) &= \mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((\delta a + 1 + b)x) \\ \mu_d(x) &= \mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((\delta(a+1) + b)x). \end{aligned}$$

Define

$$\begin{aligned} S_{\psi_d}(\delta) &= N_{\psi_d}(0) - N_{\psi_d}(1) && (10) \\ S_{\mu_d}(\delta) &= N_{\mu_d}(0) - N_{\mu_d}(1). && (11) \end{aligned}$$

It is clear that the mapping $\psi_d(x)$ is balanced if and only if $S_{\psi_d}(\delta) = 0$.

In order to derive $R_{a,b}(\delta)$, we have to compute $N_{\psi_d}(0)$, $N_{\psi_d}(1)$, and $N_{\mu_d}(1)$ from $S_{\psi_d}(\delta)$ and $S_{\mu_d}(\delta)$.

**Case 1)** $a \neq b$ :

For $\delta = 1$, we have

$$S_{\psi_d}(1) = S_{\mu_d}(1) = \sum_{x \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((b+1+a)x)}.$$

From the linearity and balance property of $\mathrm{tr}_1^n(x)$, we have

$$S_{\psi_d}(1) = S_{\mu_d}(1) = 0.$$

From Lemma 1, we have

$$R_{a,b}(1) = -1.$$

Next we consider the case of $\delta \in F_{2^n} \setminus F_2$. For a Boolean function $k(x)$ on $F_{2^n}$, we can define a trace transform $K(\lambda)$ given by

$$K(\lambda) = \sum_{x \in F_{2^n}} (-1)^{k(x) + \mathrm{tr}_1^n(\lambda x)}.$$

It is obvious that $S_{\psi_d}(\delta)$ and $S_{\mu_d}(\delta)$ in (10) and (11) are the values of trace transform of the quadratic Boolean function

$$k(x) = \mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x)$$

evaluated at $\lambda = \delta a + 1 + b$ and $\lambda = \delta(a+1) + b$, respectively.

The rank of the quadratic Boolean function $k(x)$ gives its distribution of trace transform values (see Theorem 6.2 of [2]). Now we have to examine the bilinear form of $k(x)$ to compute the rank of the quadratic Boolean function $k(x)$ [4]. The bilinear form of $k(x)$ is given by

$$\begin{aligned} B_k(x,y) &= k(x) + k(y) + k(x+y) \\ &= \mathrm{tr}_1^n(x[\mathrm{tr}_1^n(\delta y) + \delta \mathrm{tr}_1^n(y)]). \end{aligned}$$

The number of $y$ which satisfies $B_k(x,y) = 0$ for all $x$ is equal to that of the solutions to the equation

$$\mathrm{tr}_1^n(\delta y) + \delta \mathrm{tr}_1^n(y) = 0.$$

Since $\delta \in F_{2^n} \setminus F_2$, the number of solutions is equal to the number of $y \in F_{2^n}$ satisfying

$$\mathrm{tr}_1^n(\delta y) = 0 \ \text{ and } \ \mathrm{tr}_1^n(y) = 0, \tag{12}$$

which is obviously $2^{n-2}$ derived from the difference-balance property of the trace function. Thus the rank of the quadratic form is $n - (n-2) = 2$.

It is not difficult to derive the values of $\lambda$ which yield nonzero $K(\lambda)$. For $\lambda = 0$,

$$K(0) = \sum_{x \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x)} = 2^{n-1}$$

because $(\mathrm{tr}_1^n(\delta x), \mathrm{tr}_1^n(x)) = (1,1)$ occurs $2^{n-2}$ times as $x$ varies over $F_{2^n}$. In a similar way, we have

$$K(\lambda) = \begin{cases} 2^{n-1}, & \lambda = 0, 1, \delta \\ -2^{n-1}, & \lambda = 1 + \delta \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

Since $S_\psi(\delta)$ and $S_\mu(\delta)$ are $K(\lambda)$ evaluated at $\lambda = \delta a + 1 + b$ and $\delta(a+1) + b$, respectively, (13) can be rewritten as

$$S_{\psi_d}(\delta) = \begin{cases} 0, & \delta \neq \frac{b+1}{a}, \frac{b}{a}, \frac{b+1}{a+1}, \frac{b}{a+1} \\ 2^{n-1}, & \delta = \frac{b+1}{a}, \frac{b}{a}, \frac{b+1}{a+1} \\ -2^{n-1}, & \delta = \frac{b}{a+1} \end{cases} \tag{14}$$

$$S_{\mu_d}(\delta) = \begin{cases} 0, & \delta \neq \frac{b}{a+1}, \frac{b+1}{a+1}, \frac{b}{a}, \frac{b+1}{a} \\ 2^{n-1}, & \delta = \frac{b}{a+1}, \frac{b+1}{a+1}, \frac{b}{a} \\ -2^{n-1}, & \delta = \frac{b+1}{a} \end{cases} \tag{15}$$

for $\delta \in F_{2^n}^*$.

Finally from (10),(11),(14), and (15), we have

$$R_{a,b}(\delta) = \begin{cases} -1 + j2^{n-1}, & \delta = \frac{b+1}{a} \\ -1 + 2^{n-1}, & \delta = \frac{b}{a} \text{ and } \frac{b+1}{a+1} \\ -1 - j2^{n-1}, & \delta = \frac{b}{a+1} \\ -1, & \text{otherwise.} \end{cases}$$

**Case 2)** $a = b$ :

When $\delta = 1$, it is straightforward that $d(x) = 0$ and $R_{1,2}(1) = 2^n - 1$. For $\delta \in F_{2^n} \setminus F_2$, we have

$$S_{\psi_d}(\delta) = \begin{cases} 2^{n-1}, & \delta = \frac{a+1}{a} \\ -2^{n-1}, & \delta = \frac{a}{a+1} \\ 0, & \text{otherwise} \end{cases} \tag{16}$$

$$S_{\mu_d}(\delta) = \begin{cases} 2^{n-1}, & \delta = \frac{a}{a+1} \\ -2^{n-1}, & \delta = \frac{a+1}{a} \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

Thus the correlation distribution is given by

$$R_{a,b}(\delta) = \begin{cases} 2^n - 1, & \delta = 1 \\ -1 + j2^{n-1}, & \delta = \frac{a+1}{a} \\ -1 - j2^{n-1}, & \delta = \frac{a}{a+1} \\ -1, & \text{otherwise} \end{cases}$$

for $\delta \in F_{2^n}^*$. □

Using Theorem 1, we can construct a set of quaternary LCZ sequences.

**Theorem 2** : Let $n$ and $e$ be positive integers such that $e|n$. Let $\beta$ be a primitive element in $F_{2^e}$ and $T = \frac{2^n-1}{2^e-1}$. Let $\mathcal{M} = \{m_i(x) | 0 \leq i \leq 2^e - 2,\ x \in F_{2^n}^*\}$ be the set of sequences defined by the functions

$$\begin{aligned} m_0(x) &= 2\mathrm{tr}_1^n(x) \\ m_i(x) &= \mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(\beta^i x), \quad \text{for } 1 \leq i \leq 2^e - 2. \end{aligned}$$

Then, the set $\mathcal{M}$ is a $(2^n-1, 2^e-1, T, 1)$ LCZ sequence set and has the following correlation distribution:

$$R_{i,k}(\delta) = \begin{cases} 2^n-1, & 2^e-1 \text{ times} \\ -1, & A \text{ times} \\ -1+j2^{n-1}, & 2^e(2^e-2) \text{ times} \\ -1-j2^{n-1}, & 2^e(2^e-2) \text{ times} \\ -1+2^{n-1}, & 2(2^e-1)(2^e-2) \text{ times} \\ 2^{n-1}-1+j2^{n-1}, & 2(2^e-1) \text{ times} \\ 2^{n-1}-1-j2^{n-1}, & 2(2^e-1) \text{ times} \end{cases} \tag{18}$$

as $\delta$ varies over $F_{2^n}^*$ and $0 \le i,k \le 2^e-2$ and where $A$ is $2+(2^{n+e}+2^n-5\cdot 2^e+4)(2^e-1)$.

*Proof :* Set $\delta = \alpha^\tau$. Let $d(x) = m_i(\delta x) - m_k(x)$. We consider the following five cases.

**Case 1)** $i = k = 0$ (once):

In this case, $R_{0,0}(\delta)$ can be rewritten as

$$R_{0,0}(\delta) = \begin{cases} 2^n-1, & \text{once for } \delta = 1 \\ -1, & 2^n-2 \text{ times for } \delta \in F_{2^n} \setminus F_2. \end{cases}$$

**Case 2)** $i = k \neq 0$ ($2^e-2$ times):

Let $a = \beta^i = \beta^k$. From Theorem 1, the correlation function is given as

$$R_{i,i}(\delta) = \begin{cases} 2^n-1, & \text{once for } \delta = 1 \\ -1+j2^{n-1}, & \text{once for } \delta = \frac{a+1}{a} \\ -1-j2^{n-1}, & \text{once for } \delta = \frac{a}{a+1} \\ -1, & \text{otherwise } (2^n-4 \text{ times}) \end{cases}$$

for $\delta \in F_{2^n}^*$.

**Case 3)** $i \neq 0$ and $k = 0$ ($2^e-1$ times) :

Set $a = \beta^i$. Then $d(x)$ is given by $d(x) = \{\mathrm{tr}_1^n(\delta x) \boxplus 2\mathrm{tr}_1^n(a\delta x)\} - 2\mathrm{tr}_1^n(x)$. Thus $R_{i,0}(\delta)$ is written as

$$R_{i,0}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{\mathrm{tr}_1^n(\delta x) \boxplus 2(\mathrm{tr}_1^n(a\delta x) + \mathrm{tr}_1^n(x))}.$$

It is clear that $N_{\psi_d}(0) = 2^n$ if $\delta = \frac{1}{a}$ and $2^{n-1}$ otherwise. And $N_{\mu_d}(0) = 2^n$ if $\delta = \frac{1}{a+1}$ and $2^{n-1}$ otherwise. Using Lemma 1, we have

$$R_{i,0}(\delta) = \begin{cases} 2^{n-1}-1+j2^{n-1}, & \text{once for } \delta = \frac{1}{a} \\ 2^{n-1}-1-j2^{n-1}, & \text{once for } \delta = \frac{1}{a+1} \\ -1, & \text{otherwise } (2^n-3 \text{ times}). \end{cases}$$

**Case 4)** $i = 0$ and $k \neq 0$ ($2^e-1$ times) :

Set $b = \beta^k$. Similarly to Case 3, we have

$$R_{0,k}(\delta) = \begin{cases} 2^{n-1}-1+j2^{n-1}, & \text{once for } \delta = b \\ 2^{n-1}-1-j2^{n-1}, & \text{once for } \delta = b+1 \\ -1, & \text{otherwise } (2^n-3 \text{ times}). \end{cases}$$

**Case 5)** $i \neq k$, $i \neq 0$, and $k \neq 0$ ($(2^e-1)(2^e-2)$ times ):

Let $a = \beta^i$ and $b = \beta^k$. The crosscorrelation function between the two sequences $m_i(x)$ and $m_k(x)$ is given by

$$R_{i,k}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{\left(\mathrm{tr}_1^n(x\delta) \boxplus 2\mathrm{tr}_1^n(ax\delta)\right) \boxminus \left(\mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(bx)\right)}.$$

From Theorem 1, we have

$$R_{i,k}(\delta) = \begin{cases} -1+j2^{n-1}, & \text{once for } \delta = \frac{b+1}{a} \\ -1+2^{n-1}, & \text{twice for } \delta = \frac{b}{a} \text{ or } \frac{b+1}{a+1} \\ -1-j2^{n-1}, & \text{once for } \delta = \frac{b}{a+1} \\ -1, & \text{otherwise } (2^n-5\text{times}). \end{cases}$$

Given any pair of sequences in the set $\mathcal{M}$, the correlation functions have the low correlation zone $[1-T, T-1]$. We can derive (18) by combining the above 5 cases. □

## References


[1] R. De Gaudenzi, C. Elia, and R. Viola, "Bandlimited quasisynchronous CDMA: A novel satellite access technique for mobile and personal communication systems," *IEEE J. Select. Areas Commun.*, vol. 10, pp. 328-343, Feb., 1992.

[2] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Amsterdam, The Netherlands: Elservier, 1998.

[3] S.-H. Kim, H. Chung, and J.-S. No, "New cyclic relative difference sets constructed from $d$-homogeneous functions with difference-balance property," submitted to *IEEE Trans. Inform. Theory*, Aug. 2003.

[4] S.-H. Kim and J.-S. No, "New families of binary sequences with low correlation," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3059–3065, Nov. 2003.

[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] J.-S. No, "New cyclic difference sets with Singer parameters constructed from $d$-homogeneous functions," accepted for publication in *Designs, Codes and Cryptography*, Feb. 2003.

[7] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. 30, pp. 548–553, May 1984.