Quaternary LCZ Sequences Constructed From GMW Sequences

*Sang-Hyo Kim, Ji-Woong Jang 0, Jong-Seon No, and Habong Chung
*Seoul National University, †Hongik University
{kimsh, stasera}@ecl.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 GMW 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 (QSCDMA) 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 QSCDMA system, what matters most is to have low correlation zone around origin rather than to minimize maximum nontrivial correlation value[6]. In fact, low correlation zone (LCZ) sequences show better performance than other well-known sequence sets with optimal correlation property. Let \( S \) be a set of \( M \) sequences of period \( N \). If the magnitude of correlation function between any two sequences in \( S \) takes the values than or equal to \( \epsilon \) within the range \(-L < \tau < L\), of the offset \( \tau \), then \( S \) 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 GMW 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 \( \text{tr}_{m/n}^n(\cdot) \) from \( F_{2^n} \) to \( F_{2^m} \) is defined by \( \text{tr}_{m/n}^n(x) = \sum_{i=0}^{n-1} x^{2^i} \), where \( x \in F_{2^n} \) and \( m/n \) is well known that \( \text{tr}_{m/n}^n(\alpha^i) \) is a binary m-sequence of period \( 2^m - 1 \), 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 \( \oplus \) 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 \( \alpha^i \), then we can obtain a sequence \( s(\alpha^i) \), \( 0 \leq i \leq 2^n - 2 \), of period \( 2^n - 1 \). Hence, for convenience, we will use the expression 'a binary or quaternary sequence \( s(\alpha^i) \) 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 \( s_1(x) \) and \( s_2(x) \) is defined as

\[
R_{1,2}(\delta) = \sum_{x \in F_{2^n}} \omega_4^{s_1(x) - s_2(x)}
\]

where \( \omega_4 \) 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

\[
v = v_1 \oplus 2v_2.
\]

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

\[
v(x) = v_1(x) \oplus 2v_2(x), \quad w(x) = w_1(x) \oplus 2w_2(x)
\]
Table 1: Truth tables for \( \phi(v - w) \) and \( \psi(v - w) \).

<table>
<thead>
<tr>
<th>( \phi(v - w) )</th>
<th>( w = (0,0) )</th>
<th>( (0,1) )</th>
<th>( (1,0) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( v = (0,0) )</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(0,1)</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(1,1)</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(1,0)</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( \psi(v - w) )</th>
<th>( w = (0,0) )</th>
<th>( (0,1) )</th>
<th>( (1,0) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( v = (0,0) )</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(0,1)</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(1,1)</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(1,0)</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

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

\[
\phi(d(x)) = v_1(x) + w_1(x)
\]

\[
\psi(d(x)) = v_1(x)v_1(x) + w_1(x) + w_2(x) + v_2(x).
\]

III. Construction of Quaternary LCZ Sequences

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

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

\[
\sum_{x \in F_2^n} \omega_4^s(x) = (N_{\psi_s}(0) - N_{\mu_s}(1)) + j(N_{\mu_s}(1) - N_{\psi_s}(1)).
\]

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

\[
q(x) = f(x) \oplus 2f(ax)
\]

where \( a \in F_2^n \setminus F_2 \). Kim, Jang, No, and Chung proposed the following two theorems about quaternary LCZ sequences constructed from binary m-sequences[4].

Theorem 1 (Kim, Jang, No, and Chung[4]): Let \( m_a(x) \) and \( m_b(x) \) be two quaternary sequences defined by the functions

\[
m_a(x) = \text{tr}_4^n(x) \oplus 2\text{tr}_4^n(ax)
\]

\[
m_b(x) = \text{tr}_4^n(x) \oplus 2\text{tr}_4^n(bx)
\]

where \( a, b \in F_2^n \setminus F_2 \). Then, their crosscorrelation values are given as

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

where \( j = \sqrt{-1} \).

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

Theorem 2 (Kim, Jang, No, and Chung[4]): Let \( n \) and \( e \) be positive integers such that \( e \mid n \). Let \( \beta \) be a primitive element in \( F_2^n \) and \( T = \frac{2^n - 1}{2 - 1} \). Let \( M = \{m_i(x)\mid 0 \leq i \leq 2^e - 2, \ x \in F_2^n\} \) be the set of sequences defined by the functions

\[
m_0(x) = 2\text{tr}_4^n(x)
\]

\[
m_i(x) = \text{tr}_4^n(x) \oplus 2\text{tr}_4^n(\beta^ix), \quad \text{for} \ 0 \leq i \leq 2^e - 2.
\]

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

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

as \( \delta \) varies over \( F_2^n \) and \( 0 \leq i, k \leq 2^n - 2 \) and where \( A \) is

\[
2 + (2^{n+e} + 2^n - 5 \cdot 2^e + 4)(2^e - 1).
\]
The quaternary LCZ sequences in the set $\mathcal{M}$ are constructed with m-sequences as their constituent sequences. In this section, we apply the same method to construct the set $\mathcal{G}$ of quaternary LCZ sequences from GMW sequences. It has the same correlation property and low correlation zone as those of $\mathcal{M}$.

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

$$H(yx) = y^d H(x).$$ (6)

Lemma 2: Let $m, c$, and $n$ be positive integers such that $n = cm$. Let $q = 2^e$ and $A = \{1, a, \cdots, a^{d-1}\}$, where $a$ is a primitive element in $F_{2^e}$ and $T = \frac{q^m-1}{q-1}$.

Let $v(x)$ be a 1-form function from $F_{q^m}$ onto $F_q$ with balance and difference-balance property. For a given $\delta \in F_{q^m} \setminus F_q$, let $M_\delta(a, b)$ be the number of $x_2 \in A$ satisfying

$$v(\delta x_2) = a \quad \text{and} \quad v(x_2) = b, \quad a, b \in F_q.$$ (7)

Then, we have

$$M_\delta(0, 0) = q^{m-2} - 1 = \frac{2^{m-2} - 1}{q - 1},$$ (8)

$$M_\delta(c, 0) = \sum_{c \in F_q^*} M_\delta(0, c) = q^{m-2} - 2^{m-2},$$ (9)

$$M_\delta(cd, d) = q^{m-2} - 2^{m-2}, \quad \text{for any} \quad c \in F_q^*.$$ (10)

Proof: Let $N_\delta(a, b)$ be the number of $x \in F_{q^m}^*$ satisfying $v(\delta x) = a$ and $v(x) = b$. Let $x = x_1 x_2$, where $x_1 \in F_q$ and $x_2 \in A$. Because $v(x)$ is difference-balanced, $v(\delta x) - v(cx) = v(\delta x) - cv(x)$ is balanced for any $c \in F_q^*$ and $0$ occurs $q^{m-1} - 1$ times as $x$ varies over $F_{q^m}^*$. Thus we have

$$\sum_{a \in F_q} N_\delta(ca, a) = q^{m-1} - 1.$$ (11)

Since $v(x)$ is balanced, we have

$$\sum_{a \in F_q} N_\delta(a, 0) = \sum_{b \in F_q} N_\delta(0, b) = q^{m-1} - 1.$$ (12)

Also, note that

$$\sum_{a \in F_q} \sum_{b \in F_q} N_\delta(a, b) = q^m - 1.$$ (13)

Now, we have

$$\sum_{a \in F_q} \sum_{b \in F_q} N_\delta(a, b) = \sum_{a \in F_q} N_\delta(a, 0) + \sum_{b \in F_q} N_\delta(0, b)$$

$$- N_\delta(0, 0) + \sum_{g \in F_q^*} \sum_{a \in F_q^*} N_\delta(a, ca)$$

$$= \sum_{a \in F_q} N_\delta(a, 0) + \sum_{b \in F_q} N_\delta(0, b) - N_\delta(0, 0)$$

$$+ \sum_{g \in F_q^*} \left\{ \sum_{a \in F_q} N_\delta(a, ca) - N_\delta(0, 0) \right\}.$$ (14)

Plugging (8), (9), and (10) into (12), we have

$$N_\delta(0, 0) = q^{m-2} - 1.$$ (15)

From (8) and (13), we also have

$$\sum_{a \in F_q^*} N_\delta(ca, a) = \sum_{a \in F_q^*} N_\delta(ca, a) - N_\delta(0, 0) = q^{m-2}(q-1).$$ (16)

Let $\beta = a_T$. For a given $x_2$ such that $v(\delta x_2) = cv(x_2)$, the ordered pair $(v(\delta x), v(x)) = (x_1 v(\delta x_2), x_1 v(x_2))$ takes the each value in the list

$$(c, 1), (c\beta, \beta), \cdots, (c\beta^{q-2}, \beta^{q-2})$$

exactly once as $x_1$ varies over $F_q$. Therefore we have

$$\sum_{a \in F_q^*} N_\delta(ca, a) = (q - 1) \sum_{a \in F_q^*} M_\delta(ca, a),$$

which, in turn, tells us that

$$\sum_{a \in F_q^*} M_\delta(ca, a) = q^{m-2}.$$ (17)

Similarly, we have

$$M_\delta(0, 0) = \frac{N_\delta(0, 0)}{q - 1} = \frac{q^{m-2} - 1}{q - 1},$$ (18)

$$M_\delta(c, 0) = \frac{\sum_{a \in F_q^*} N_\delta(0, a)}{q - 1} = \frac{q^{m-2}}{q - 1},$$ (19)

$$M_\delta(0, c) = \frac{\sum_{a \in F_q^*} N_\delta(0, a)}{q - 1} = \frac{q^{m-2}}{q - 1}.$$ (20)

Theorem 3: Let $m$ and $n$ be positive integers such that $c|m$ and $T = \frac{2^e-1}{2^e-1}$. Let $r$ be an integer such that $\gcd(r, 2^e-1) = 1$ and $1 \leq r \leq 2^e-2$. Let $g(x)$ be the GMW sequence defined by

$$g(x) = tr^r((tr^r(x))').$$
Let us define the family $G = \{g_i(x)\}_{0 \leq i \leq 2^n - 2, \ x \in F_2^n}\}$ of quaternary sequences defined by

\[
\begin{align*}
g_0(x) &= 2tr_t^i([ttr_{x}^n(x)]') \\
g_i(x) &= tr_t^i([ttr_{x}^n(x)]') \oplus 2tr_t^i([\beta tr_{x}^n(x)]'),
\end{align*}
\]

where $\beta$ is a primitive element in $F_2$. Then, $G$ has the same correlation distribution as that of $M$ and is a $(2^n - 1, 2^n - 1, T, 1)$ LCZ sequence set.

**Proof:** What we are going to show is that there is a one-to-one correspondence between $M$ and $G$ so that the correlation distribution of any given pair of sequences in $G$ is identical to that of corresponding two sequences in $M$. Also we will show that the sequences $m_{ri}(x)$ of $M$ given in (19) is the one that corresponds to the sequence $g_i(x)$ of $G$ given in (15). Let $a = \beta^i$ and $b = \beta^k$. For nonzero $i$ and $k$, we have

\[
\begin{align*}
m_{ri}(x) &= tr_t^i(x) \oplus 2tr_t^i(a^r x) \\
m_{rk}(x) &= tr_t^i(x) \oplus 2tr_t^i(b^k x)
\end{align*}
\]

and

\[
\begin{align*}
g_i(x) &= tr_t^i([tr_{x}^n(x)]') \oplus 2tr_t^i([\alpha tr_{x}^n(x)]') \\
g_k(x) &= tr_t^i([tr_{x}^n(x)]') \oplus 2tr_t^i([\beta tr_{x}^n(x)]').
\end{align*}
\]

And $m_0(x)$ corresponds to $g_0(x)$. Let $A = \{\alpha^i, \alpha^i, \alpha^2, \ldots, \alpha^{T-1}\}$. For $\delta' = (\delta_1, \delta_2)$ and $\delta'' = (\delta_1', \delta_2')$, such that $\delta_1 \in F_2^n$ and $\delta_2 \in A$, define

\[
\begin{align*}
R_m(\delta') &= \sum_{x \in F_2^n} \omega_4^{m_i(\delta(x)) - m_0(x)} \\
R_g(\delta) &= \sum_{x \in F_2^n} \omega_4^{g_i(\delta(x)) - g_0(x)}.
\end{align*}
\]

Now we are going to investigate into the values of $R_g(\delta)$ from those of $R_m(\delta')$ given in Theorem 2. We have to consider the following cases:

**Case 1**) $i \neq k, i \neq 0$, and $k \neq 0$:

i) $tr_t^a(\delta x_2) \neq 0$ and $tr_t^b(\delta x_2) \neq 0$

By substituting $x = x_1 x_2$, $\delta = \delta_1 \delta_2$, such that $x_1, \delta_1 \in F_2^n$ and $x_2, \delta_2 \in A$, we can rewrite $R_m(\delta')$ and $R_g(\delta)$ as

\[
\begin{align*}
R_m(\delta') &= \sum_{x_1 \in A} \sum_{x_2 \in F_2^n} \omega_4^{tr_t^i(x_1 \delta_1') [tr_t^a(\delta_2 x_2)]'} \\
&\quad \times \omega_4^{tr_t^i(x_1 \delta_1' a'[tr_t^b(\delta_2 x_2)]')} \\
&\quad \times \omega_4^{tr_t^i(x_1 [tr_t^a(\delta_2 x_2)]') \oplus tr_t^i(x_1 [tr_t^b(\delta_2 x_2)]')} \quad (16)
\end{align*}
\]

and

\[
\begin{align*}
R_g(\delta) &= \sum_{x_1 \in A} \sum_{x_2 \in F_2^n} \omega_4^{tr_t^i(x_1 \delta_1') [tr_t^a(\delta_2 x_2)]'} \\
&\quad \times \omega_4^{tr_t^i(x_1 \delta_1' a'[tr_t^b(\delta_2 x_2)]')} \\
&\quad \times \omega_4^{tr_t^i(x_1 [tr_t^a(\delta_2 x_2)]') \oplus tr_t^i(x_1 [tr_t^b(\delta_2 x_2)]')} \quad (17)
\end{align*}
\]

For a given $x_2$, let $\xi_{x_2} = tr_t^a(\delta x_2)$ and $\xi_{x_2} = tr_t^a(\delta x_2)$. Then the inner summation of (16) is rewritten as

\[
\sum_{x_1 \in F_2^n} \omega_4^{tr_t^i(x_1 \delta_1') \oplus tr_t^i(x_1 \delta_1' a')} = \sum_{x_1 \in F_2^n} \omega_4^{tr_t^i(x_1 \delta_1') \oplus tr_t^i(x_1 \delta_1' a')},
\]

which is the crosscorrelation $R_{a, a'}(\delta')$ of two quaternary sequences of period $2^n - 1$, namely $tr_t^i(x_1) \oplus 2tr_t^i(a' x_1)$ and $tr_t^i(x_1) \oplus 2tr_t^i(b' x_1)$. Similarly, we can see the inner summation of (17) is nothing but $R_{a, a'}(\delta')$. Thus, we have

\[
\sum_{x_1 \in F_2^n} \omega_4^{tr_t^i(x_1 \delta_1') \oplus tr_t^i(x_1 \delta_1' a')} = \sum_{x_1 \in F_2^n} \omega_4^{tr_t^i(x_1 \delta_1') \oplus tr_t^i(x_1 \delta_1' a')},
\]

ii) $tr_t^a(\delta x_2) = 0$ or $tr_t^b(\delta x_2) = 0$

In this case, it is easy to derive that

\[
\sum_{x_1 \in F_2^n} \omega_4^{m_i(\delta(x)) - m_0(x)} = \sum_{x_1 \in F_2^n} \omega_4^{m_i(\delta(x)) - m_0(x)}.
\]

**Case 2**) $i = 0, k = 0$:

This is the case of the autocorrelation of binary m-sequences for $R_m(\delta')$ and GMW sequences for $R_g(\delta)$.

**Case 3**) $i = k \neq 0$:

This is the case of autocorrelation. From Theorem 1, we have $R_m(\delta') = R_g(\delta)$.

**Case 4**) $i \neq 0$ and $k = 0$ (or $i = 0$ and $k \neq 0$):

In this case, only one quaternary sequence remains in the exponent of $\omega_4$. It is easily checked that $R_m(\delta) = R_g(\delta)$.

Consequently, we have $R_m(\delta') = R_g(\delta)$. Therefore, $G$ is a $(2^n - 1, 2^n - 1, T, 1)$ LCZ sequence set.

References


