\( p^2 \)-ary LCZ Sequences Constructed From \( p \)-ary Extended Sequences

\(^{1}\)Ji-Woong Jang, Jong-Seon No, and Habong Chung

\(^{1}\)Seoul National University, Hongik University

Abstract

In this paper, given a composite integer \( n \), we propose a method of constructing \( p \)-ary low correlation zone (LCZ) sequences of period \( p^n - 1 \) from \( p \)-ary \( m \)-sequences of the same length. The new construction method is a generalized form of the quaternary LCZ sequence by Kim, Jang, No, and Chung in the view of the alphabet size. The correlation distribution of these new \( p \)-ary LCZ sequences is derived.

I. Introduction

In the area of wireless LAN where the cell size is very small, the time delay in the reverse link within a few chip due to the relatively small delay of transmission. The quasi-synchronous code-division multiple-access (QS-CDMA) system proposed by Gaudenzi, Elia, and Vilola\(^{1}\) allows multiple chip time delay among different users, which gives more flexibility in designing the wireless communication system.

In the design of sequences for QS-CDMA system, it is important to have low correlation zone around origin 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 \( S \) be a set of \( M \) sequences of period \( N \). If the magnitude of correlation function between any two sequences in \( S \) takes the values less 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 \( p \)-ary low correlation zone (LCZ) sequences of period \( p^n - 1 \) from \( p \)-ary \( m \)-sequences of the same length. The new construction method is a generalized form of the quaternary LCZ sequence by Kim, Jang, No, and Chung\(^{3}\) in the view of the alphabet size. The correlation distribution of these new \( p \)-ary LCZ sequences is derived.

II. Preliminaries

In this section, we introduce some definitions and notations.

\(^{1}\)This work was supported in part by BK21 and ITRC program.
Let \( f(x) \) be a mapping from \( F_{p^n} \) onto \( F_p \), where \( e|n \). The function \( f(x) \) is said to be balanced if each nonzero element of \( F_{p^n} \) appears \( p^{n-e} \) times and zero element \( p^{n-e} - 1 \) times in the list \( \{ f(x) | x \in F_{p^n} \} \). A function \( f(x) \) is said to be difference-balanced if \( f(\delta x) - f(x) \) is balanced for any \( \delta \in F_{p^n} \setminus \{0,1 \} \). It is pointed out in [2] and [6] that the binary sequence with difference-balance property has the ideal auto-correlation property necessarily and sufficiently.

### III. Construction of \( p^2 \)-ary LCZ Sequences

In this section, for a prime \( p \), we construct a set of \( p^2 \)-ary LCZ sequences using a \( p \)-ary extended sequence with the same period as their constituent sequences.

Let \( f(x) \) be a function from \( F_{p^n} \) to \( F_p \). We can use \( f(x) \) as the constituent sequence of a \( p^2 \)-ary sequence \( q(x) \) as

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

where \( a \in F_{p^n} \setminus F_p \). Most of sequences in this paper are constructed in this manner. Klapper [?] introduced the \( d \)-form function. A \( d \)-form function \( H(x) \) on \( F_{p^n} \) over \( F_p \) is defined as a function satisfying for any \( y \in F_{p^n} \) and \( x \in F_p \),

\[
H(yx) = y^dH(x).
\] (1)

**Lemma 1 (Kim, Jang, No, and Chung[3])**

Let \( m, c, \) and \( n \) be positive integers such that \( n = em \).

Let \( q = p^r \) and \( A = \{1, \alpha, \cdots, \alpha^{r-1}\} \), where \( \alpha \) is a primitive element of \( F_{p^n} \) and \( T = (q^n - 1)/(q - 1) \). Let \( v(x) \) be a \( 1 \)-form function from \( F_{p^n} \) onto \( F_q \) with balance and difference-balance property. For a given \( \delta \in F_{p^n} \setminus F_q \), let \( M_{\delta}(a,b) \) be the number of \( x_2 \in A \) satisfying

\[
v(\delta x_2) = a \text{ and } v(x_2) = b, \ a, b \in F_q.
\] (2)

Then, we have

\[
M_0(0,0) = q^{m-2} - 1 \quad q - 1 \quad p^{n-2e} - 1 \quad p^e - 1
\]

\[
\sum_{c \in F_q} M_{\delta}(c,0) = \sum_{c \in F_q} M_0(0,c) = q^{m-2} = p^{n-2e}
\]

\[
\sum_{d \in F_q} M_{\delta}(cd,d) = q^{m-2} = p^{n-2e} \text{ for any } c \in F_q^*.
\]

No, Yang, Chung, and Song constructed extended sequences with ideal autocorrelation property from sequences of short period with ideal autocorrelation property [7]. We use the extended sequences to construct LCZ sequence sets.

**Theorem 1 (No, Yang, Chung, and Song[7])**

Let \( n \) and \( e \) be positive integers such that \( e|n \). Let \( f(x) \) be the function from \( F_{p^n} \) to \( F_p \) with difference-balance property such that \( f(0) = 0 \). Let \( r \) be an integer such that \( \gcd(r, p^e - 1) = 1 \) and \( 1 \leq r \leq p^e - 2 \), then the sequence of period \( 2^n - 1 \) defined by

\[
f(\delta x^e)^r)
\]

has the ideal autocorrelation property.

\[
\square
\]

Using the \( p \)-ary extended sequences form in above theorem, we can construct LCZ sequences as in the following theorem.

**Theorem 2**

Let \( n \) and \( e \) be positive integers such that \( e|n \). Let \( f(x) \) be the function from \( F_{p^n} \) to \( F_p \) with difference-balance property such that \( f(0) = 0 \). Let \( r \) be an integer such that \( \gcd(r, p^e - 1) = 1 \) and \( 1 \leq r \leq p^e - 2 \). Let \( \beta \) be a primitive element in \( F_{p^n} \).

Let \( H = \{ h_a(x) | a \in F_{p^n} \setminus \{0\} \} \) be the set of \( p^e - 1 \) \( p^2 \)-ary sequences defined by the functions

\[
h_0(x) = pf(\delta x^e)^r)
\]

\[
h_a(x) = f(\delta x^e)^r) \oplus pf(\alpha^e \delta x^e)^r), \ a \in F_{p^n} \setminus F_p.
\]

Then, \( H \) is a \( (p^n - 1, p^e - p + 1, \frac{p^{n-1}}{p^e - 1} - 1) \) \( p^2 \)-ary LCZ sequence set.

**Proof**

Consider two sequences in \( H \) given by

\[
h_1(x) = f(\delta x^e)^r) \oplus pf(\alpha^e \delta x^e)^r)
\]

\[
h_k(x) = f(\delta x^e)^r) \oplus pf(\beta^e \delta x^e)^r)
\]

In the computation of the correlation function \( R_{a,b}(\delta) \) between the above two sequences, we have to consider the following cases:

**Case 1** \( a \neq 0, b \neq 0, \) and \( a \neq b \):

Then \( R_{a,b}(\delta) \) is given by

\[
R_{a,b}(\delta) = \sum_{x \in F_{p^n}} \sum_{y \in F_{p^n}} \omega_p^{h_1(\delta x) - h_k(x)}
\]

\[
\sum_{x \in A} \sum_{x \in F_{p^n}} \omega_p^{f(x)^r)} \delta x^e)^r) \oplus pf(\alpha^e \delta x^e)^r)
\]

For \( \delta \notin F_{p^n} \), with the replacement of \( \delta x^e \) by \( cd \) and \( \delta x^e \) by \( d \) and also from Lemma 1, \( R_{a,b}(\delta) \)
is rewritten as

\[ R_{a,b}(\delta) = \sum_{d \in F_p} M_d(0,0) \sum_{x_1 \in F_p} \sum_{x_2 \in F_p} \omega_{p^2} \left\{ f\left( [x_1d]^r \right) \otimes pf\left( [x_1ac]^r \right) \right\} \]

Therefore, \( R_{a,b}(\delta) \) for \( \delta \in F_{p^2} \) can be rewritten as follows

\[ R_{a,b}(\delta) = \sum_{y \in F_{p^2}} N(y) \omega_{p^2} \left\{ f(\delta y) \otimes pf(a^s \delta^r) - (f(y) \otimes pf(b^s \delta^r)) \right\} + p^{n-\varepsilon} \]
By the result in [6], it is clear that \( R_{0,0}(1) = -1. \)

**Case 4** \( a = b = 0: \)

Obviously, \( R_{0,0}(1) = p^n - 1. \) When \( \delta \neq 1, \) from the difference balance property of extended sequence, it is clear that \( R_{0,0}(\delta) = -1. \)

From the above 4 cases, the correlation function \( R_{a,b}(\delta) \) takes the value \(-1\) in the low correlation zone \( \delta \in \{ \alpha^{-T+1}, \ldots, 1, \ldots, \alpha^{T-1}\} \) except for the in-phase autocorrelation value.

\( \square \)

**Example 1:** Let \( p = 3, n = 4, e = m = 2, \) and \( T = (3^n - 1)/(3^3 - 1) = 10. \) Let \( \alpha \) be a primitive element in \( F_{3^4} \) and \( \beta = \alpha^T. \) Then the following set \( M \) is the 9-ary LCZ sequences set with parameter \((80, 7, 10, 1).\)

\[
\mathcal{M} = \{ m_\alpha(x) | x = \alpha \in F_{3^4} \cup \{0\}\}
\]

where \( m_\alpha(x) = m_i(\alpha^x) \) is given as

\[
\begin{align*}
m_0(\alpha^x) &= p \text{tr}^1_1(\alpha^x) \\
&= 0000000660036006360036363606 \\
&= 0666330663003603363636603363 \\
&= 006306036036033660360363636036 \\
m_0(\alpha^x) &= \text{tr}^1_1(\alpha^x) \oplus p \text{tr}^1_1(\alpha^x) \\
&= 836663237556072676844508 \\
&= 6585211402542463310614167577 \\
&= 30513534887043747122801781
\end{align*}
\]

\[
\begin{align*}
m_{\alpha^2}(\alpha^x) &= \text{tr}^1_1(\alpha^x) \oplus p \text{tr}^1_1(\alpha^x) \\
&= 26338062867553078373211502 \\
&= 352584410851813664031434577 \\
&= 60546561227016717488204724
\end{align*}
\]

\[
\begin{align*}
m_{\alpha^4}(\alpha^x) &= \text{tr}^1_1(\alpha^x) \oplus p \text{tr}^1_1(\alpha^x) \\
&= 86335068565123015313844208 \\
&= 3285774024543667043737211 \\
&= 60276264881046141755807187
\end{align*}
\]

\[
\begin{align*}
m_{\alpha^8}(\alpha^x) &= \text{tr}^1_1(\alpha^x) \oplus p \text{tr}^1_1(\alpha^x) \\
&= 563320652624883042343577805 \\
&= 385821170287273661037131844 \\
&= 6081686754076474122501451
\end{align*}
\]

References


