p^2-ary LCZ Sequences Constructed From p-ary Extended Sequences
1

*Ji-Woong Jang O, *Jong-Seon No, and +Habong Chung
*Seoul National University, +Hongik University
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 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 nonntrivial 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 ϵ within the range $-L < \tau < L$, of the offset τ, then $\mathcal{S}$ is called an (N, M, L, ϵ) 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.

Let p be a prime and F_{p^n} be the finite field with p^n elements. The trace function $\mathrm{tr}_m^n(\cdot)$ from F_{p^n} to F_{p^m} is defined by

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

where $x \in F_{p^n}$ and $m|n$. The trace function has the following properties.

(i) $\mathrm{tr}_m^n(ax+by) = a\,\mathrm{tr}_m^n(x) + b\,\mathrm{tr}_m^n(y)$, for all $a, b \in F_{p^m}$, $x, y \in F_{p^n}$

(ii) $\mathrm{tr}_m^n(x^{2^m}) = \mathrm{tr}_m^n(x)$, for all $x \in F_{p^n}$.

It is well known that $\mathrm{tr}_1^n(\alpha^t)$ is a p-ary m-sequence of period $p^n - 1$, where α is a primitive element in F_{p^n}.

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

Let $F_{p^n}^* = F_{p^n} \backslash \{0\}$ and $s(x)$ be a mapping from F_{p^n} to F_p or Z_{p^2}. If we restrict the mapping $s(x)$ to $F_{p^n}^*$ and replace x by α^t, then we can obtain a sequence $s(\alpha^t)$, $0 \le t \le p^n - 2$, of period $p^n - 1$. Hence, for convenience, we will use the expression 'a $p-$ary or p^2-ary sequence $s(\alpha^t)$ of period $p^n - 1$' interchangeably with 'a mapping $s(x)$ from F_{p^n} to F_p or Z_{p^2}'.

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

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

where w_{p^2} is a complex p^2th root of unity.

[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^e}, where $e|n$. The function $f(x)$ is said to be *balanced* if each nonzero element of F_{p^e} 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 $\delta \in F_{p^n}\backslash\{0,1\}$. It is pointed out in [2] and [6] that the binary sequence with difference-balance property has the ideal autocorrelation 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

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

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^e} is defined as a function satisfying for any $y \in F_{p^e}$ and $x \in F_{p^n}$

$$H(yx) = y^d H(x). \tag{1}$$

Lemma 1 (Kim, Jang, No, and Chung[3]) : Let m, e, and n be positive integers such that $n = em$. Let $q = p^e$ and $A = \{1, \alpha, \cdots, \alpha^{T-1}\}$, where α is a primitive element of F_{p^n} and $T = (q^m-1)/(q-1)$. 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

$$v(\delta x_2) = a \ \text{ and } \ v(x_2) = b, \quad a,b \in F_q. \tag{2}$$

Then, we have

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

□

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^e} 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 $1 \le r \le p^e-2$, then the sequence of period 2^n-1 defined by

$$f([\mathrm{tr}_e^n(x)]^r)$$

has the ideal autocorrelation property.

□

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^e} 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 $1 \le r \le p^e-2$. Let β be a primitive element in F_{p^e}. Let $\mathcal{H} = \{h_a(x) \mid a \in F_{p^e}\backslash F_p \cup \{0\}\}$ be the set of p^e-1 p^2-ary sequences defined by the functions

$$\begin{aligned}
h_0(x) &= pf([\mathrm{tr}_e^n(x)]^r) \\
h_a(x) &= f([\mathrm{tr}_e^n(x)]^r) \boxplus pf([a\mathrm{tr}_e^n(x)]^r), \quad a \in F_{p^e}\backslash F_p.
\end{aligned}$$

Then, $\mathcal{H}$ 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 $\mathcal{H}$ given by

$$\begin{aligned}
h_i(x) &= f([\mathrm{tr}_e^n(x)]^r) \boxplus pf(a^r[\mathrm{tr}_e^n(x)]^r) \\
h_k(x) &= f([\mathrm{tr}_e^n(x)]^r) \boxplus pf(b^r[\mathrm{tr}_e^n(x)]^r)
\end{aligned}$$

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

Case 1) $a \ne 0$, $b \ne 0$, and $a \ne b$:

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

$$\begin{aligned}
R_{i,k}(\delta) =& \sum_{x \in F_{p^n}^*} \omega_{p^2}^{h_i(\delta x) - h_k(x)} \\
=& \sum_{x_2 \in A} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\left\{f(x_1^r[\mathrm{tr}_e^n(\delta x_2)]^r) \boxplus pf(x_1^r a^r [\mathrm{tr}_e^n(\delta x_2)]^r)\right\}} \\
& \times \omega_{p^2}^{-\left\{f(x_1^r[\mathrm{tr}_e^n(x_2)]^r) \boxplus pf(x_1^r b^r [\mathrm{tr}_e^n(x_2)]^r)\right\}}.
\end{aligned}$$

For $\delta \notin F_{p^e}$, with the replacement of $\mathrm{tr}_e^n(\delta x_2)$ by cd and $\mathrm{tr}_e^n(x_2)$ by d and also from Lemma 1, $R_{a,b}(\delta)$

is rewritten as

$$R_{a,b}(\delta) = \sum_{d\in F^*_{p^e}} M_\delta(cd,d) \sum_{c\in F^*_{p^e}} \sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{\{f([x_1cd]^r)\boxplus pf([x_1acd]^r)\}-\{f([x_1d]^r)\boxplus pf([x_1bd]^r)\}}$$
$$+M_\delta(0,0)\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^0$$
$$+\sum_{c\in F^*_{p^e}} M_\delta(c,0)\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{\{f([x_1c]^r)\boxplus pf([x_1ac]^r)\}}$$
$$+\sum_{c\in F^*_{p^e}} M_\delta(0,c)\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{-\{f([x_1c]^r)\boxplus pf([x_1bc]^r)\}}$$
$$= p^{n-2e}\sum_{c\in F^*_{p^e}}\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{\{f([x_1cd]^r)\boxplus pf([x_1acd]^r)\}} \times\omega_{p^2}^{-\{f([x_1d]^r)\boxplus pf([x_1bd]^r)\}} + p^{n-2e}-1$$
$$+p^{n-2e}\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{\{f([x_1c]^r)\boxplus pf([x_1ac]^r)\}}$$
$$+p^{n-2e}\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{-\{f([x_1c]^r)\boxplus pf([x_1bc]^r)\}}$$
$$= p^{n-2e}\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{-\{f([x_1d]^r)\boxplus pf([x_1bd]^r)\}} \times\sum_{c\in F^*_{p^e}} \omega_{p^2}^{\{f([x_1cd]^r)\boxplus pf([x_1acd]^r)\}} + p^{n-2e}-1$$
$$+p^{n-2e}\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{\{f([x_1c]^r)\boxplus pf([x_1ac]^r)\}}$$
$$+p^{n-2e}\sum_{x_1\in F^*_{p^e}} \omega_{p^2}^{-\{f([x_1c]^r)\boxplus pf([x_1bc]^r)\}} -1.$$

Let $I_f(a) = \sum_{x\in F^*_{p^e}} w_{p^2}^{f(x^r)\boxplus pf([ax]^r)}$, then we get the following equation.

$$\begin{aligned} R_{a,b}(\delta) &= p^{n-2e}(I_f(a)I^*_f(b)+1+I_f(a)+I^*_f(b)) \\ &= p^{n-2e}(1+I_f(a))(1+I^*_f(b))-1 \qquad (3)\end{aligned}$$

where $*$ means complex conjugate.

From the result in [6], $I_f(a)=I^*_f(b)=-1$, for all $a,b\in F_{p^e}\backslash F_p$. Therefore, $R_{a,b}(\delta)=-1$, for all $\delta\in F_{p^n}\backslash F_{p^e}$.

For $\delta\in F_{p^e}$, $R_{a,b}(\delta)$ is given as follows

$$\begin{aligned} R_{a,b}(\delta) &= \sum_{x\in F^*_{p^n}} \omega_{p^2}^{\left\{f([\mathrm{tr}^n_e(\delta x)]^r)\boxplus pf([\mathrm{tr}^n_e(a\delta x)]^r)\right\}} \\ &\quad\times\omega_{p^2} - \{f([\mathrm{tr}^n_e(x)]^r)\boxplus pf([\mathrm{tr}^n_e(bx)]^r)\} \\ &= \sum_{x\in F^*_{p^n}} \omega_{p^2}^{\left\{f(\delta^r[\mathrm{tr}^n_e(x)]^r)\boxplus pf(a^r\delta^r[\mathrm{tr}^n_e(x)]^r)\right\}} \\ &\quad\times\omega_{p^2}^{-\left\{f([\mathrm{tr}^n_e(x)]^r)\boxplus pf(b^r[\mathrm{tr}^n_e(x)]^r)\right\}}.\end{aligned}$$

Let $N(a)$ be the nunmber of $x\in F_{p^n}$, such that $\mathrm{tr}^n_e(x)=a$. Since $\mathrm{tr}^n_e(x)$ has balance property, $N(a)$ has the following values

$$N(a)=\begin{cases} p^{n-e}-1, & \text{if } a=0\\ p^{n-e}, & \text{otherwise.}\end{cases}$$

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

$$\begin{aligned} R_{a,b}(\delta) &= \sum_{y\in F_{p^e}} N(y)\omega_{p^2}^{\{f(\delta^r y)\boxplus pf(a^r\delta^r y)\}-\{f(y)\boxplus pf(b^r y)\}} \\ &= p^{n-e}\sum_{y\in F^*_{p^e}} \omega_{p^2}^{\{f(\delta^r y)\boxplus pf(a^r\delta^r y)\}-\{f(y)\boxplus pf(b^r y)\}} \\ &\quad +p^{n-e}-1 \\ &= p^{n-e}(C_{a^r,b^r}(\delta^r)+1)-1 \qquad (4)\end{aligned}$$

where $C_{a,b}(\delta)=\sum_{y\in F^*_{p^e}} \omega_{p^2}^{\{f(\delta y)\boxplus pf(a\delta y)\}-f(y)\boxplus pf(by)\}}$. When $\delta=1$, it is clear that above equation is equal to -1.

Case 2) $a=b\neq 0$:

When $\delta\notin F_{p^e}$, the correlation function is given as

$$\begin{aligned} R_{a,a}(\delta) &= p^{n-2e}(I_f(a)I^*_f(a)+1+I_f(a)+I^*_f(a))-1 \\ &= p^{n-2e}(1+I_f(a))(1+I^*_f(a)) \\ &= -1.\end{aligned}$$

For $\delta\in F_{p^e}$, by the similar process to case 1), we have

$$R_{a,a}(\delta)=p^{n-e}(C_{a^r,a^r}(\delta^r)+1)-1.$$

It is clear that $R_{a,a}(1)=p^n-1$. For $\delta\in F_{p^e}\backslash\{1\}$, $R_{a,a}(\delta)=-1$.

Case 3) $a=0$ and $b\neq 0$(or $a=0$ and $b\neq 0$):

For $\delta\notin F_{p^e}$, by the similar way in case 1), $R_{0,b}(\delta)$ is given as follows

$$\begin{aligned} R_{0,b}(\delta) &= p^{n-2e}(I_f(0)I^*_f(b)+1+I_f(0)+I^*_f(b)) \\ &= p^{n-2e}(1+I_f(0))(1+I^*_f(b)) \\ &= -1.\end{aligned}$$

where $I_f(0)=\sum_{x\in F^*_{p^e}} \omega_{p^2}^{pf(x)}$.

For $\delta\in F_{p^2}$, by the similar process to case 2) $R_{0,b}(\delta)$ is given as follows

$$R_{0,b}(\delta) = p^{n-e}(C_{0,b^r}(\delta^r)+1)-1$$

where $C_{0,b}(\delta) = \sum_{y\in F^*_{p^e}} \omega_{p^2}^{\{pf(a\delta y)\}-f(y)\boxplus pf(by)\}}$. When $\delta=1$, it is clear that above equation is equal to -1.

By the result in [6], it is clear that $R_{0,b}(1) = -1$.

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 $\delta \in \{\alpha^{-T+1}, \cdots, 1, \cdots, \alpha^{T-1}\}$ except for the in-phase autocorrelation value.

□

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

$$\mathcal{M} = \{m_a(x) \mid a \in F_{3^2} \backslash F_3 \cup \{0\}\}$$

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

$$\begin{aligned}
m_0(\alpha^t) &= p\ \mathrm{tr}_1^4(\alpha^t) \\
&= 600060066063660036030633606 \\
&\quad\ 066663330663630003003303633 \\
&\quad\ 00630603663030333366603363 \\
m_{\alpha^T}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^T \alpha^t) \\
&= 836620382327556072676844508 \\
&\quad\ 658521140254246331064161577 \\
&\quad\ 30513534887043747122801781 \\
m_{\alpha^{2T}}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{2T} \alpha^t) \\
&= 263380628687553078373211502 \\
&\quad\ 352584410851813664031434577 \\
&\quad\ 60546561227016717488204724 \\
m_{\alpha^{3T}}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{3T} \alpha^t) \\
&= 863350685651223015313844208 \\
&\quad\ 328257740524543667034737211 \\
&\quad\ 60276264881046141755807187 \\
m_{\alpha^{5T}}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{5T} \alpha^t) \\
&= 563320652624883042343577805 \\
&\quad\ 385821170287273661037131844 \\
&\quad\ 60816867554076474122501451 \\
m_{\alpha^{6T}}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{6T} \alpha^t) \\
&= 236650325354886045646211802 \\
&\quad\ 682857710581516337061767844 \\
&\quad\ 30873831224013414755207427 \\
m_{\alpha^{7T}}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{7T} \alpha^t) \\
&= 536680358381226018616577205 \\
&\quad\ 625284470827876334067464211 \\
&\quad\ 30243237551073171488504154
\end{aligned}$$

□

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] 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.

[3] S.-H. Kim, J.W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1469-1477, April 2005.

[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] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proc. IEEE Int. Symp. Inform. Theory and Its Appl. (ISITA'96)*, Victoria, British Columbia, Canada, Sept. 1996, pp. 837–840.

[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,* 2005.