New Optimal p-ary Low Correlation Zone Sequences[1]

*Ji-Woong Jang[O], *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, for integers n and e such that $e|n$ and $2^e - 1$ is a prime, we propose a method of constructing binary low correlation zone (LCZ) sequences of period $2^n - 1$ by using the extended form sequence with the same period. These new LCZ sequences use Legendre sequences as their column sequences.

1. Introduction

In the quasi-synchronous CDMA system [1] where maintaining synchronization within a few chips is feasible even in the reverse link due to the relatively small transmission delay, the most important property of the sequences used for reducing multiple access interference (MAI) is low correlation property around the origin [6]. Long, Zhang, and Hu [6] proposed the sequence set that has low correlation value around the origin, which can be used as a spreading sequence in the quasi-synchronous CDMA system. The sequence set with this property is called *low correlation zone (LCZ) sequence*. They also have shown that an LCZ sequence set has better performance than other well-known sequence sets with optimal correlation property [6]. For a prime p, Tang and Fan [10] proposed p-ary LCZ sequence sets by extending the alphabet size of each sequence in Long's work [6]. And they also proposed a construction method of p-ary LCZ sequence sets by using interleaved sequences [11]. Kim, Jang, No, and Chung proposed a new construction method of quaternary LCZ sequence sets by using binary sequence of the same period with ideal autocorrelation and they also calculated the correlation distributions of their sequence sets constructed from m-sequence and GMW sequence [4]. Their quaternary LCZ sequence set is optimal with respect to the bound by Tang, Fan, and Matsufuji [12]. But for a prime p, no optimal set of p-ary LCZ sequence set has been reported yet.

In this paper, we propose new construction methods of constructing optimal LCZ sequences. We construct the new p-ary LCZ sequence sets by adopting p-ary sequence of period $p^m - 1$ with ideal autocorrelation for integers n and m such that $m|n$ as a column sequence. The new construction methods give us the optimal sets with respect to the bound by Tang, Fan, and Matsufuji [12].

[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.

2. Preliminaries

In this section, we introduce some definitions and notations.

Let $\mathcal{S}$ be a set of D 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 for the offset τ in the range $-Z < \tau < Z$, then $\mathcal{S}$ is called an (N, D, Z, ϵ) LCZ sequence set.

Let p be a prime and F_{p^n} be the finite field with p^n elements. Let $v_i(x)$ and $v_j(x)$ be two p-ary sequences of period $p^n - 1$, defined in $F_{p^n}^* = F_{p^n} \backslash \{0\}$. Then for $\delta \in F_{p^n}^*$, the correlation function between two p-ary sequences $v_i(x)$ and $v_j(x)$ is defined as

$$R_{v_i,v_j}(\delta) = \sum_{x \in F_{p^n}^*} \omega_p^{v_i(x\delta) - v_j(x)}$$

where ω_p is a complex primitive p-th root of unity. We will abuse the notation of the correlation function as $R_{i,j}(\tau) = R_{v_i,v_j}(\alpha^\tau)$ for $\delta = \alpha^\tau$, where α is a primitive element in F_{p^n}.

Let $v(t)$ be a p-ary sequence of period $p^n - 1$. Then $v(t)$ is said to have balance property if number of zero element is one less than that of each nonzero element in one period of the sequence. And if the sequence $v(t) - v(t + \tau)$ is balanced for all $\tau \not\equiv 0 \bmod p^n - 1$, then $v(t)$ is said to have difference-balance property.

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 $m|n$.

Klapper [5] introduced the d-form function. A d-form function $H(x)$ on F_{p^n} over F_{p^m} is defined as a function satisfying for any $y \in F_{p^m}$ and $x \in F_{p^n}$

$$H(yx) = y^d H(x). \quad (1)$$

Tang and Fan [11] stated the following theorem using the interleaved sequence [2], which can be used for the construction of an LCZ sequence set.

Theorem 1 [Tang and Fan [11]] Let m and n be integers such that $m|n$. Let $f(y)$ and $g(y)$ be cyclically distinct sequences of period p^m-1 from F_{p^m} to F_p and the function $h(x)$ from F_{p^n} to F_{p^m} be a 1-form function over F_{p^m} with balance and difference-balance property. If we set $f(0)=g(0)=0$, then the correlation function $R_{f,g}(\delta)$ between $f(h(x))$ and $g(h(x))$ is given as

$$R_{f,g}(\delta)=\sum_{x\in F_{p^n}^*}\omega_p^{f(h(\delta x))-g(h(x))}$$
$$=\begin{cases}p^{n-m}\big(C_{f,g}(\delta)+1\big)-1, & \text{if } \delta\in F_{p^m}\\ p^{n-2m}(I(f)+1)(\bar{I}(g)+1)-1, & \text{if } \delta\notin F_{p^m}\end{cases}$$

where $I(f)=\sum_{y\in F_{p^m}^*}\omega_p^{f(y)}$, $C_{f,g}(\delta)=\sum_{y\in F_{p^m}^*}\omega_p^{f(\delta y)-g(y)}$, and $\bar{I}(\cdot)$ denotes complex conjugate of $I(\cdot)$. □

In the above theorem, $f(\cdot)$ and $g(\cdot)$ are called the *column sequences* of period p^m-1 in the two dimensional representation of the sequences $f(h(\cdot))$ and $g(h(\cdot))$ of period p^n-1, respectively.

It is clear that $I(f)=-1$ corresponds to the balance property of the column sequence $f(y)$ defined on $F_{p^m}^*$ if p is a prime. If the column sequences are balanced, we have

$$R_{f,g}(\delta)=-1,\quad \text{for } \delta\notin F_{p^m}.$$

In order to have $R_{f,g}(1)=-1$, we have to have $C_{f,g}(1)=-1$, which means that the in-phase cross-correlation function of each pair in the column sequence set has the value -1.

Property 2 Let $\mathcal{A}$ be the set of sequences of period p^m-1 satisfying the following properties:

i) All the sequences in the set $\mathcal{A}$ are cyclically distinct.

ii) Each sequence in the set $\mathcal{A}$ has the balance property.

iii) In-phase cross-correlation value of each pair of the sequences in the set $\mathcal{A}$ is always -1.

□

Theorem 1 tells us that if we have the sequence set $\mathcal{A}$ satisfying Property 2, then the $(p^n-1,|\mathcal{A}|,(p^n-1)/(p^m-1),1)$ p-ary LCZ sequence set can be constructed.

In the subsequent sections, we propose methods of constructing the column sequence sets satisfying Property 2, some of which are of the maximum size.

3. New Optimal p-ary LCZ Sequence Sets

In this section, for a prime p and integers n and m such that $m|n$, we propose a new construction method of the optimal p-ary LCZ sequence set of period p^n-1 by using a p-ary sequence of period p^m-1 with ideal autocorrelation.

The following lemma can be easily stated without proof.

Lemma 3 Let $m_1(t)$ and $m_2(t)$ be two cyclically distinct p-ary sequences with linear span L_1 and L_2, respectively. The maximum run lengths of the symbol 0 and the symbol a, $1\le a\le p-1$, for the difference sequence $m_1(t)-m_2(t)$ are less than or equal to L_1+L_2-1 and L_1+L_2, respectively.

□

In the next theorem, we construct a set of p-ary cyclically distinct sequences of period p^m-1 satisfying Property 2 from a p-ary sequence with ideal autocorrelation.

Theorem 4 Let p be a prime and $m(t)$ be a p-ary sequence with ideal autocorrelation of period $M=p^m-1$. Let L_m be the linear span of $m(t)$ and $\{m_i(t)\mid 0\le i\le M-1\}$ be a set of cyclic shifts of $m(t)$, such that $m_i(t)=m(t+i)$, $t=0,1,2,\cdots,M-1$. Define new sequences $s_i(t)$, $0\le i\le M-1$, such that

$$s_i(t)=\begin{cases}m_i(M-1-t), & 0\le t\le M-K-1\\ m_i(t+K), & M-K\le t\le M-1\end{cases}\quad(2)$$

for some integer K in the range $3L_m-1\le K\le M/2$. Then the set of p-ary sequences $s_i(t)$, $0\le i\le M-1$ satisfies Property 2.

Proof: From the definition of $s_i(t)$, it is clear that all $s_i(t)$ are balanced and it is also easy to see that the in-phase cross-correlation $C_{s_i,s_j}(1)$ between $s_i(t)$ and $s_j(t)$ takes the value -1.

Now, what we have to show is that for any i, j, and τ, $s_j(t)=s_i(t+\tau)$ implies that $i=j$ and $\tau=0$. The sequence $s_i(t)$ in (2) can be rewritten as

$$s_i(t)=\begin{cases}m(M-1-t+i), & 0\le t\le M-K-1\\ m(t+i+K), & M-K\le t\le M-1.\end{cases}\quad(3)$$

It is not difficult to see that $s_i(t+\tau)$ can be expressed as:

Case 1) $0\le\tau\le M-K-1$

$$s_i(t+\tau)=\begin{cases}m(M-1-t-\tau+i),\\ \qquad 0\le t\le M-K-1-\tau\\ m(t+\tau+i+K),\\ \qquad M-K-\tau\le t\le M-\tau-1\\ m(M-1-t-\tau+i),\\ \qquad M-\tau\le t\le M-1.\end{cases}\quad(4)$$

Assume $s_j(t) = s_i(t+\tau)$ for all t. Then from (3) and (4), we have

$$m(M-1-t+j) = m(M-1-t-\tau+i), \quad 0 \le t \le M-K-1-\tau \tag{5}$$

$$m(M-1-t+j) = m(t+\tau+i+K), \quad M-K-\tau \le t \le M-K-1 \tag{6}$$

$$m(t+j+K) = m(t+\tau+i+K), \quad M-K \le t \le M-\tau-1 \tag{7}$$

$$m(t+j+K) = m(M-1-t-\tau+i), \quad M-\tau \le t \le M-1. \tag{8}$$

Here, we consider the following two cases depending on τ.

When $\tau \le 2L_m-1$, both $(M-K-\tau)$ and $(K-\tau)$ are greater than or equal to L_m since $3L_m-1 \le K \le M/2$. From (5), we have

$$m(M-1-t+j) - m(M-1-t-\tau+i) = 0 \tag{9}$$

for consecutive $M-K-\tau$ values of t. And similarly from (7), we have

$$m(t+j+K) - m(t+\tau+i+K) = 0 \tag{10}$$

for consecutive $K-\tau$ values of t. It is clear that the linear span of $m(t)-m(t+k)$ for all k, $1 \le k \le p^m-2$, is L_m. Since both $M-K-\tau$ and $K-\tau$ are greater than or equal to L_m, (9) and (10) imply that

$$j = i-\tau = i+\tau$$

which further tells us that $i=j$ and $\tau = 0$. And again in this case, (6) and (8) vanish.

When $\tau \ge 2L_m$, (6) or (8) implies that some consecutive τ bits of two sequences $m(t)$ and $m(-t)$ are identical, which is a contradiction from Lemma 3 since the linear span of $m(t)-m(-t+k)$ for all k, $0 \le k \le p^m-2$, is at most $2L_m$.

Case 2) $\tau \ge M-T$

In this case, $s_i(t+\tau)$ can be rewritten as

$$s_i(t+\tau) = \begin{cases} m(t+K+i+\tau), & 0 \le t \le M-1-\tau \\ m(M-t+i-1-\tau), & M-\tau \le t \le 2M-K-\tau-1 \\ m(t+K+i+\tau), & 2M-\tau-K \le t \le M-1. \end{cases}$$

Again, assuming $s_j(t) = s_i(t+\tau)$ gives us

$$m(M-1-t+j) = m(t+K+i+\tau), \quad 0 \le t \le M-1-\tau \tag{11}$$

$$m(M-1-t+j) = m(M-t+i-1-\tau), \quad M-\tau \le t \le M-K-1 \tag{12}$$

$$m(t+j+K) = m(M-t+i-1-T), \quad M-K \le t \le 2M-K-\tau-1 \tag{13}$$

$$m(t+j+K) = m(t+T+i+\tau), \quad 2M-K-\tau \le t \le M-1. \tag{14}$$

When $\tau \ge (M-K)+L_m$, both $\tau-K$ and $\tau-(M-K)$ are greater than or equal to L_m, since $M-K > K$. From (12), we have

$$m(M-1-t+j) - m(M-t+i-1-\tau) = 0$$

for consecutive $(\tau-K)$ values of t. And from (14), we have

$$m(t+j+K) - m(t+K+i+\tau) = 0$$

for consecutive $\tau-(M-K)$ values of t. Similarly to Case 1), since both $\tau-K$ and $\tau-(M-K)$ are greater than or equal to L_m, we can deduce $i=j$ and $\tau=0$.

When $\tau \le (M-K)+L_m-1$, we have $M-\tau \ge 2L_m$. Therefore, either (11) or (13) implies that some consecutive $M-\tau$ bits of two cyclically inequivalent sequences are identical, which is again a contradiction from Lemma 3. □

Note that even if we limit the range of K as $3L_m-1 \le K \le M/2$ in Theorem 4 for the sake of the simplicity of the proof, in fact the theorem holds for all K such that $3L_m-1 \le K \le M-(3L_m-1)$. If $3L_m-1 > M/2$, the above theorem cannot be directly applied. But there are many sequences with $3L_m-1 > M/2$, the set of which obtained as in Theorem 4 satisfies Property 2. For example, the sequences $s_i(t)$ in (2) constructed from the binary m-sequence with $L_m = 4$ of period $M = 15$ are all cyclically distinct for $K = 7$. The proof for such cases should be further investigated into.

Using Theorem 1 and the column sequence set in Theorem 4, we can construct the p-ary LCZ sequence sets as in the following theorem.

Theorem 5 Let p be a prime and n and m be integers such that $m|n$. Let $T = (p^n-1)/(p^m-1)$ and $M = p^m-1$. Let α be a primitive element in F_{p^n} and $\beta = \alpha^T$ be a primitive element in F_{p^m}. Let $h(x)$ from F_{p^n} to F_{p^m} be a 1-form function over F_{p^m} with balance and difference-balance property, i.e., a p^m-ary unified sequence [7] which includes an m-sequence, a GMW sequence, and a generalized GMW sequence. Let $f_i(\beta^t) = s_i(t)$, where $s_i(t)$ is the sequence defined in Theorem 4. Then the following sequence set $\mathcal{P}$ defined by

$$\mathcal{P} = \{v_i(t) = f_i(h(\alpha^t)) \mid 0 \le i \le p^m-2,\ 0 \le t \le p^n-2\}$$

is a LCZ sequence set with parameters $(p^n-1, p^m-1, T, 1)$.

□

Using Tang-Fan-Matsufuji bound given by

$$DZ - 1 \le \frac{N-1}{1-\epsilon^2/N} \tag{15}$$

we can check the optimality of our binary LCZ sequence set $\mathcal{P}$.

Corollary 6 The p-ary LCZ sequence set $\mathcal{P}$ in Theorem 5 is optimal with respect to the Tang-Fan-Matsufuji bound.

Proof: The proof is straightforward. By substituting $N = p^n - 1$, $D = p^m - 1$, and $\epsilon = 1$ in (15), we have

$$(p^m - 1)Z - 1 \leq \frac{p^n - 2}{1 - 1/(p^n - 1)}$$

and thus

$$Z \leq \frac{p^n}{p^m - 1}.$$

Since Z is an integer, we have

$$Z \leq \left\lfloor \frac{p^n}{p^m - 1} \right\rfloor = \frac{p^n - 1}{p^m - 1} = T.$$

Clearly, $\mathcal{P}$ is optimal with respect to the Tang-Fan-Matsufuji bound. □

References

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

[2] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inform. Theory*, vol. 41, pp. 400–411, Mar. 1995.

[3] J.-W. Jang, J.-S. No, and H. Chung, "New sets of optimal binary low correlation zone sequences," *Proc. 2nd Int. Workshop on Sequence Design and its Application in Commun.*, (Shimonoseki, Yamaguchi, Japan), Oct. 10–14, 2005, pp. 73–77.

[4] 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.

[5] A. Klapper, "d-form sequence: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423–431, Mar. 1995.

[6] 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.

[7] J.-S. No, "p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation property," *IEEE Trans. Inform. Theory*, vol. 48, no. 9, pp. 2540–2546, Sept. 2002.

[8] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inform. Theory,* vol. 42, no. 6, pp. 2254–2255, Nov. 1996.

[9] 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.

[10] 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.

[11] 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,* 2004.

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

[13] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.