IEICE TRANS. FUNDAMENTALS, VOL.E89–A, NO.10 OCTOBER 2006

PAPER Special Section on Information Theory and Its Applications

A New Construction of Optimal p^2-Ary Low Correlation Zone Sequences Using Unified Sequences**

Ji-Woong JANG[†*], *Nonmember*, **Jong-Seon NO**[†a)], *Member*, *and* **Habong CHUNG**[††], *Nonmember*

SUMMARY In this paper, given an integer e and n such that $e|n$, and a prime p, we propose a method of constructing optimal p^2-ary low correlation zone (LCZ) sequence set with parameters $(p^n-1, p^e-1, (p^n-1)/(p^e-1), 1)$ from a p-ary sequence of the same length with ideal autocorrelation. The resulting p^2-ary LCZ sequence set can be viewed as the generalization of the optimal quaternary LCZ sequence set by Kim, Jang, No, and Chung in respect of the alphabet size. This generalization becomes possible due to a completely new proof comprising any prime p. Under this proof, the quaternary case can be considered as a specific example for $p = 2$.

key words: *low correlation zone (LCZ) sequences, p^2-ary sequences, quasi-synchronous code division multiple access (QS-CDMA), unified sequences*

1. Introduction

In the reverse link of the mobile radio communication systems, each user has different time delay and thus the synchronous code division multiple access (CDMA) cannot be adopted as a multiple access scheme in such systems. But in the microcellular system such as the wireless local area network (LAN), where the cell size is very small and the time delay can be maintained within a few chips, the quasi-synchronous code division multiple access (QS-CDMA) system can be used. In the QS-CDMA system, the spreading sequences having low correlation values for the time shift of a few chips around origin are needed, which are called *low correlation zone (LCZ) sequences*.

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. Long, Zhang, and Hu [1] proposed a binary LCZ sequence set by using a GMW sequence [2]. For a prime p, Tang and Fan [3] proposed p-ary LCZ sequences by extending the alphabet size of each sequence in Long's work [1]. And they also constructed p-ary LCZ sequences by using interleaved sequences [4]. Recently, Kim, Jang, No, and Chung proposed quaternary LCZ sequence sets constructed from a binary sequence with ideal autocorrelation [5]. The set of these sequences is optimal with respect to the bound by Tang, Fan, and Matsufuji [6].

In this paper, given an integer e and n such that $e|n$, and a prime p, we propose a method of constructing optimal p^2-ary LCZ sequence set with parameters $(p^n-1, p^e-1, (p^n-1)/(p^e-1), 1)$ from a p-ary sequence of the same length with ideal autocorrelation. The resulting p^2-ary LCZ sequence set can be viewed as the generalization of the optimal quaternary LCZ sequence set by Kim, Jang, No, and Chung [5] in respect of the alphabet size. This generalization becomes possible due to a completely new proof comprising any prime p. Under this proof, the quaternary case can be considered as a specific example for $p = 2$ [5].

2. Preliminaries

Let p be a prime and F_{p^n} 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 as

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

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) $\mathrm{tr}_m^n(x^{p^m}) = \mathrm{tr}_m^n(x)$, 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 are dealing 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}, when 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 domain of $s(x)$ 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 correlation function between two p^2-ary sequences $s_i(x)$ and $s_j(x)$ is defined as

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

Manuscript received February 6, 2006.
Manuscript revised March 27, 2006.
Final manuscript received May 9, 2006.

[†]The authors are with the School of Electrical Engineering and Computer Science, Seoul National University, Korea.
[††]The author is with the School of Electronics and Electrical Engineering, Hongik University, Korea.
[*]Presently, with Samsung Electronics.

**This paper was supported by ITRC and Laboratory of Excellency Program.

a) E-mail: jsno@snu.ac.kr

DOI: 10.1093/ietfec/e89–a.10.2656

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

Let e and n be integers such that $e|n$ and let $v(x)$ be a mapping from F_{p^n} onto F_{p^e}. The function $v(x)$ 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 $\{v(x)|\ x \in F_{p^n}^*\}$. A function $v(x)$ is said to be *difference-balanced* if $v(\delta x) - v(x)$ is balanced for any $\delta \in F_{p^n}\backslash\{0,1\}$. Let $f(x)$ be a function from F_{p^n} to F_p. We can build a p^2-ary sequence $s_a(x)$ using $f(x)$ as the constituent sequence of $s_a(x)$ as shown below:

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

where $a \in F_{p^e}^*$. Most of LCZ sequences in this paper are constructed in this manner.

3. p^2-Ary LCZ Sequences Constructed from Unified Sequences

In this section, for a prime p, we construct a set of p^2-ary LCZ sequences using a p-ary unified sequence [7] as their constituent sequence.

A d-form function $h(x)$ on F_{p^n} over F_{p^m} [8] is defined as a function satisfying for any $y \in F_{p^m}$ and $x \in F_{p^n}$ such that $m|n$

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

As pointed out in [8], a d-form function with difference-balance property plays an important role in designing sequences with ideal autocorrelation. The following lemma can be given from the proof of Theorem 2 in [9].

Lemma 1 (Kim, No, Chung, and Helleseth [9]): Any d-form function $h(x)$ from F_{p^n} to F_{p^m} with difference-balance property is 2-tuple balanced, i.e., for $\delta \in F_{p^n}\backslash F_{p^m}$, $(h(x), h(\delta x)) = (0,0)$ appears $p^{n-2m}-1$ times and $(h(x), h(\delta x)) = (a,b)$ appears p^{n-2m} times for each nonzero (a,b) as x varies over $F_{p^n}^*$. □

It is clear that any d-form function $h(x)$ from F_{p^n} to F_{p^m} with difference-balance property is balanced and $h(0) = 0$.

Using a d-form function, No [7] constructed unified sequences with ideal autocorrelation from sequences of shorter period with ideal autocorrelation as in the following theorem.

Theorem 1 (No [7]): Let e and n be positive integers such that $e|n$. Let $f(\cdot)$ be a 1-form function from F_{p^e} to F_p with difference-balance property. Let $v(\cdot)$ be a 1-form function from F_{p^n} to F_{p^e} with difference-balance property. For an integer r, $1 \le r \le p^e-2$, relatively prime to p^e-1, the p-ary unified sequence $u(x)$ of period p^n-1 defined by

$$u(x) = f([v(x)]^r) \tag{2}$$

has the ideal autocorrelation property. □

In general, Theorem 1 holds for any d-form function $v(x)$ satisfying $(d, p^e-1) = 1$ and for any d-form function $f(x)$ such that $(d, p-1) = 1$.

For some index set I, the most typical example of the 1-form function has the following expression

$$\sum_{k\in I} b_k \mathrm{tr}_1^e(y^k), \quad \text{for } y \in F_{p^e}^*, b_k \in F_p^*, \quad k \equiv 1 \bmod (p-1). \tag{3}$$

Thus if the p-ary sequence of period p^e-1 in (3) has the ideal autocorrelation, it can serve as $f(\cdot)$ in Theorem 1. Let $e|n$ and $l \equiv 1 \bmod p^e-1$ for all l in some index set J. Similarly, the most typical example of $v(x)$ in Theorem 1 can be expressed as

$$v(x) = \sum_{l\in J} c_l \mathrm{tr}_e^n(x^l), \quad \text{for } x \in F_{p^n}^*, c_l \in F_p^*, l \equiv 1 \mod (p^e-1), \tag{4}$$

provided that the p-ary sequence of period p^n-1 given by

$$\sum_{l\in J} c_l \mathrm{tr}_1^n(x^l), \quad \text{for } x \in F_{p^n}^*, c_l \in F_p^*$$

has the ideal autocorrelation property. Then the unified sequence $u(x)$ in Theorem 1 can be written as

$$u(x) = \sum_{k\in I} b_k \mathrm{tr}_1^e\Big(\Big[\sum_{l\in J} c_l \mathrm{tr}_e^n(x^l)\Big]^{kr}\Big). \tag{5}$$

The p-ary unified sequences include p-ary m-sequences, p-ary GMW sequences, p-ary d-form sequences, and p-ary extended sequences as their special cases. When $J = \{1\}$ in (4), $u(x)$ in (5) is called the p-ary extended sequence. Additionally, if $I = \{1\}$ in (3), then $u(x)$ becomes the p-ary GMW sequence.

Using the unified sequences in the above theorem, we can construct LCZ sequences as in the following theorem. The next lemma is needed for the proof of the theorem.

Lemma 2 (Kim, Jang, No, and Chung [5]): Let p be a prime and e and n be positive integers such that $e|n$. Let $A = \{1, \alpha, \cdots, \alpha^{T-1}\}$, where α is a primitive element in F_{p^n} and $T = (p^n-1)/(p^e-1)$. Let $v(x)$ be a 1-form function from F_{p^n} onto F_{p^e} with difference-balance property. For a given $\delta \in F_{p^n}\backslash F_{p^e}$, let $M_\delta(a,b)$ be the number of $x_2 \in A$ satisfying

$$v(\delta x_2) = a \ \text{ and } \ v(x_2) = b, \quad a, b \in F_{p^e}. \tag{6}$$

Then, we have

$$M_\delta(0,0) = \frac{p^{n-2e}-1}{p^e-1}$$
$$\sum_{c\in F_{p^e}^*} M_\delta(c,0) = \sum_{c\in F_{p^e}^*} M_\delta(0,c) = p^{n-2e}$$
$$\sum_{d\in F_{p^e}^*} M_\delta(cd,d) = p^{n-2e} \quad \text{for any } c \in F_{p^e}^*.$$

□

Theorem 2: Let e and n be positive integers such that $e|n$ and r be an integer such that $(p^e-1, r) = 1$ and $1 \le r \le$

$p^e - 2$. Let $T = (p^n - 1)/(p^e - 1)$. Let $f(\cdot)$ and $v(\cdot)$ be the functions defined in Theorem 1. Define the $p^e - 1$ p^2-ary sequences $s_a(x)$ of period $p^n - 1$ as

$$s_a(x) = \begin{cases} pf([av(x)]^r), & \text{for } a \in F_p^* \\ f([v(x)]^r) \boxplus pf([av(x)]^r), & \text{for } a \in F_{p^e} \backslash F_p. \end{cases}$$

Then the set $\mathcal{S}$ of p^2-ary sequences given by

$$\mathcal{S} = \{s_a(x) \mid a \in F_{p^e}^*,\ x \in F_{p^n}^*\}$$

is a p^2-ary LCZ sequence set with parameters $(p^n - 1, p^e - 1, T, 1)$.

Proof : Let α be a primitive element in F_{p^n} and $A = \{1, \alpha, \alpha^2, \cdots, \alpha^{T-1}\}$. Although the low correlation zone of the above sequence set is $[-T + 1, T - 1]$, what we are going to prove is that the correlation function $R_{a,b}(\delta)$ of $s_a(x)$ and $s_b(x)$ takes the value -1 for all $\delta \in \{1\} \cup F_{p^n} \backslash F_{p^e}$ and for all $a, b \in F_{p^e}^*$. Then the following five separate cases should be considered.

Case 1) $a, b \in F_p^*$:

The correlation function $R_{a,b}(\delta)$ can be rewritten as

$$\begin{aligned} R_{a,b}(\delta) &= \sum_{x \in F_{p^n}^*} \omega_{p^2}^{\{pf([av(\delta x)]^r)\} \boxminus \{pf([bv(x)]^r)\}} \\ &= \sum_{x \in F_{p^n}^*} \omega_{p^2}^{p\{f([av(\delta x)]^r) - f([bv(x)]^r)\}} \\ &= \sum_{x \in F_{p^n}^*} \omega_p^{f([av(\delta x)]^r) - f([bv(x)]^r)}. \end{aligned}$$

Since the unified sequence $f([v(x)]^r)$ is difference-balanced, $f([av(\delta x)]^r) - f([bv(x)]^r) \mod p$ is balanced except for $\delta = b/a$. Thus we have $R_{a,b}(\delta) = -1$ for all $\delta \in F_{p^n}^* \backslash \{b/a\}$.

Case 2) $a, b \in F_{p^e} \backslash F_p$ and $\delta \in F_{p^n} \backslash F_{p^e}$:

Let $x = x_1 x_2$, where $x \in F_{p^n}$, $x_1 \in F_{p^e}$, and $x_2 \in A$. Then the correlation function $R_{a,b}(\delta)$ of $s_a(x)$ and $s_b(x)$ is given as

$$\begin{aligned} R_{a,b}(\delta) &= \sum_{x \in F_{p^n}^*} \omega_{p^2}^{s_a(\delta x) \boxminus s_b(x)} \\ &= \sum_{x_2 \in A} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\left\{f(x_1^r [v(\delta x_2)]^r) \boxminus f(x_1^r [v(x_2)]^r)\right\}} \\ &\quad \times \omega_{p^2}^{\left\{pf(x_1^r a^r [v(\delta x_2)]^r) \boxminus pf(x_1^r b^r [v(x_2)]^r)\right\}}. \end{aligned} \tag{7}$$

Let $v(\delta x_2) = cd$ and $v(x_2) = c$ for $v(\delta x_2) \neq 0$ and $v(x_2) \neq 0$. From Lemma 2, $R_{a,b}(\delta)$ is rewritten as

$$\begin{aligned} R_{a,b}(\delta) &= \sum_{c \in F_{p^e}^*} \sum_{d \in F_{p^e}^*} M_\delta(cd, d) \\ &\quad \times \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\{f([x_1 cd]^r) \boxminus f([x_1 d]^r)\}} \\ &\quad \times \omega_{p^2}^{\{pf([x_1 acd]^r) \boxminus pf([x_1 bd]^r)\}} \\ &\quad + M_\delta(0,0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^0 \\ &\quad + \sum_{c \in F_{p^e}^*} M_\delta(c, 0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1 c]^r) \boxplus pf([x_1 ac]^r)} \\ &\quad + \sum_{c \in F_{p^e}^*} M_\delta(0, c) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1 c]^r) \boxplus pf([x_1 bc]^r)\}} \\ &= \sum_{c \in F_{p^e}^*} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\{f([x_1 c]^r) \boxplus pf([x_1 ac]^r)\}} \\ &\quad \times \omega_{p^2}^{-\{f([x_1]^r) \boxplus pf([x_1 b]^r)\}} \sum_{d \in F_{p^e}^*} M_\delta(cd, d) \\ &\quad + M_\delta(0,0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^0 \\ &\quad + \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1]^r) \boxplus pf([x_1 a]^r)} \sum_{c \in F_{p^e}^*} M_\delta(c, 0) \\ &\quad + \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \boxplus pf([x_1 b]^r)\}} \sum_{c \in F_{p^e}^*} M_\delta(0, c) \\ &= p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \sum_{c \in F_{p^e}^*} \omega_{p^2}^{\{f([x_1 c]^r) \boxplus pf([x_1 ac]^r)\}} \\ &\quad \times \omega_{p^2}^{-\{f([x_1]^r) \boxplus pf([x_1 b]^r)\}} \\ &\quad + p^{n-2e} - 1 + p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1]^r) \boxplus pf([x_1 a]^r)} \\ &\quad + p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \boxplus pf([x_1 b]^r)\}} \\ &= p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \boxplus pf([x_1 b]^r)\}} \\ &\quad \times \sum_{c \in F_{p^e}^*} \omega_{p^2}^{f([c]^r) \boxplus pf([ac]^r)} + p^{n-2e} - 1 \\ &\quad + p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1]^r) \boxplus pf([x_1 a]^r)} \\ &\quad + p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \boxplus pf([x_1 b]^r)\}}. \end{aligned}$$

Let $I_f(a) = \sum_{x_1 \in F_{p^e}^*} w_{p^2}^{f([x_1]^r) \boxplus pf([ax_1]^r)}$. Then we have

$$\begin{aligned} R_{a,b}(\delta) &= p^{n-2e}(I_f(a)\overline{I_f(b)} + 1 + I_f(a) + \overline{I_f(b)}) - 1 \\ &= p^{n-2e}(1 + I_f(a))(1 + \overline{I_f(b)}) - 1 \end{aligned} \tag{8}$$

where $\overline{I_f(b)}$ denotes complex conjugate of $I_f(b)$. From Lemma 1, for $a \in F_{p^e} \backslash F_p$, 2-tuples $(f(x_1), f(ax_1))$ are balanced, which means that $f([x_1]^r) \boxplus pf([ax_1]^r) \mod p^2$ is balanced as x_1 varies over $F_{p^e}^*$. Thus we have $I_f(a) = \overline{I_f(b)} = -1$ for all $a, b \in F_{p^e} \backslash F_p$. Therefore, $R_{a,b}(\delta) = -1$ for all $\delta \in F_{p^n} \backslash F_{p^e}$.

Case 3) $a, b \in F_{p^e} \backslash F_p$, $a \neq b$ and $\delta = 1$:

Let $N(y)$ be the number of $x \in F_{p^n}^*$ such that $v(x) = y$. Since any d-form function with difference-balance property is balanced, we have

$$N(y) = \begin{cases} p^{n-e} - 1, & \text{if } y = 0 \\ p^{n-e}, & \text{otherwise.} \end{cases} \tag{9}$$

Then $R_{a,b}(1)$ can be rewritten as

$$\begin{aligned} R_{a,b}(1) &= \sum_{y\in F_{p^e}} N(y)\omega_{p^2}^{\{f(y)\boxplus pf(a^r y^r)\}\boxminus\{f(y)\boxplus pf(b^r y^r)\}} \\ &= p^{n-e}\sum_{y\in F_{p^e}} \omega_{p^2}^{p\{f(a^r y^r)-f(b^r y^r)\}} - 1 = -1. \end{aligned}$$

Case 4) $a \in F_{p^e}\backslash F_p$, $b \in F_p^*$ (or $a \in F_p^*$, $b \in F_{p^e}\backslash F_p$), and $\delta \in F_{p^n}\backslash F_{p^e}$:

Similarly to Case 2), the correlation function $R_{a,b}(\delta)$ in (7) can be rewritten as

$$\begin{aligned} R_{a,b}(\delta) &= \sum_{x_2\in A}\sum_{x_1\in F_{p^e}^*} \omega_{p^2}^{\left\{f(x_1^r[v(\delta x_2)]^r)\boxplus pf(x_1^r a^r[v(\delta x_2)]^r)\right\}} \\ &\quad\times \omega_{p^2}^{-\left\{pf(x_1^r[bv(x_2)]^r)\right\}} \\ &= \sum_{c\in F_{p^e}^*}\sum_{d\in F_{p^e}^*} M_\delta(cd,d) \\ &\quad\times \sum_{x_1\in F_{p^e}^*} \omega_{p^2}^{\{f([x_1cd]^r)\boxplus pf([x_1acd]^r)\}\boxminus\{pf([x_1bd]^r)\}} \\ &\quad + M_\delta(0,0)\sum_{x_1\in F_{p^e}^*}\omega_{p^2}^{0} \\ &\quad + \sum_{c\in F_{p^e}^*} M_\delta(c,0)\sum_{x_1\in F_{p^e}^*}\omega_{p^2}^{f([x_1c]^r)\boxplus pf([x_1ac]^r)} \\ &\quad + \sum_{c\in F_{p^e}^*} M_\delta(0,c)\sum_{x_1\in F_{p^e}^*}\omega_{p^2}^{-pf([x_1bc]^r)} \\ &= p^{n-2e}\sum_{x_1\in F_{p^e}^*}\omega_p^{-f([bx_1]^r)}\sum_{c\in F_{p^e}^*}\omega_{p^2}^{f([c]^r)\boxplus pf([ac]^r)} \\ &\quad + p^{n-2e} - 1 + p^{n-2e}\sum_{x_1\in F_{p^e}^*}\omega_{p^2}^{f([x_1]^r)\boxplus pf([x_1a]^r)} \\ &\quad + p^{n-2e}\sum_{x_1\in F_{p^e}^*}\omega_p^{-f([x_1b]^r)}. \end{aligned}$$

Let $J_f(b) = \sum_{x_1\in F_{p^e}^*} w_p^{f([bx_1]^r)}$. Then we have

$$R_{a,b}(\delta) = p^{n-2e}(1 + I_f(a))(1 + \overline{J_f(b)}) - 1.$$

Clearly, $I_f(a) = \overline{J_f(b)} = -1$ and thus we have $R_{a,b}(\delta) = -1$ for all $\delta \in F_{p^n}\backslash F_{p^e}$.

Case 5) $a \in F_{p^e}\backslash F_p$, $b \in F_p^*$ (or $a \in F_p^*$, $b \in F_{p^e}\backslash F_p$), and $\delta = 1$:

Using $N(y)$ in (9), $R_{a,b}(1)$ can be rewritten as

$$\begin{aligned} R_{a,b}(1) &= \sum_{y\in F_{p^e}} N(y)\omega_{p^2}^{\{f(y)\boxplus pf(a^r y)\}\boxminus\{pf(b^r y)\}} \\ &= p^{n-e}\sum_{y\in F_{p^e}} \omega_{p^2}^{\{f(y)\boxplus pf(a^r y)\}\boxminus\{pf(b^r y)\}} - 1 \\ &= p^{n-e}\sum_{y\in F_{p^e}} \omega_{p^2}^{\{(1\boxplus p(p-b^r))f(y)\boxplus pf(a^r y)\}} - 1. \end{aligned} \quad (10)$$

Let $f(y) = u$ and $f(ay) = v$. Again, since 2-tuples $(f(y), f(a^r y))$ are balanced as y varies over F_{p^e}, (10) can be rewritten as

$$R_{a,b}(1) = p^{n-2e}\sum_{u\in F_p}\omega_{p^2}^{(p(p-b^r)+1)u}\sum_{v\in F_p}\omega_{p^2}^{pv} - 1.$$

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

□

Using the specific examples of $f(y)$ and $v(x)$ given in (3) and (4), Theorem 2 can be restated as follows.

Corollary 1: Let e and n be positive integers such that $e|n$ and r be an integer such that $\gcd(r, p^e - 1) = 1$ and $1 \le r \le p^e - 2$. Let $T = (p^n - 1)/(p^e - 1)$. Assume that for some index set I, the p-ary sequence of period $p^e - 1$ given by

$$\sum_{k\in I} b_k \mathrm{tr}_1^e(y^k), \quad \text{for } y \in F_{p^e}^*, b_k \in F_p^*, \quad k \equiv 1 \bmod (p-1)$$

has the ideal autocorrelation property. Let $l \equiv 1 \bmod p^e - 1$ for all l in some index set J. Assume that the p-ary sequence of period $p^n - 1$ given by

$$\sum_{l\in J} c_l \mathrm{tr}_1^n(x^l), \quad \text{for } x \in F_{p^n}^*, c_l \in F_p^*$$

also has the ideal autocorrelation property. Then the set of $p^e - 1$ p^2-ary sequences of period $p^n - 1$ defined by

$$\mathcal{S} = \{s_a(x) \mid a \in F_{p^e}^*,\ x \in F_{p^n}^*\}$$

is a p^2-ary LCZ sequence set with parameters $(p^n - 1, p^e - 1, T, 1)$, where

$$\begin{aligned} s_a(x) &= p\sum_{k\in I} b_k \mathrm{tr}_1^e\Big(\Big[a\sum_{l\in J} c_l \mathrm{tr}_e^n(x^l)\Big]^r\Big), \\ &\quad \text{for } a \in F_p^* \\ s_a(x) &= \sum_{k\in I} b_k \mathrm{tr}_1^e\Big(\Big[\sum_{l\in J} c_l \mathrm{tr}_e^n(x^l)\Big]^r\Big) \\ &\quad \boxplus p\sum_{k\in I} b_k \mathrm{tr}_1^e\Big(\Big[a\sum_{l\in J} c_l \mathrm{tr}_e^n(x^l)\Big]^r\Big), \\ &\quad \text{for } a \in F_{p^e}\backslash F_p. \end{aligned}$$

□

Tang, Fan, and Matsufuji [6] derived the upper bound on the low correlation zone and the size of an LCZ sequence set using the Welch bound [10].

Theorem 3 (Tang, Fan, and Matsufuji [6]): For an LCZ sequence set with parameters (N, M, L, ϵ),

$$ML - 1 \le \frac{N-1}{1-\epsilon^2/N}. \quad (11)$$

□

Now, we can check the optimality of p^2-ary LCZ sequence set $\mathcal{S}$ in Theorem 2.

Corollary 2: The p^2-ary LCZ sequence set $\mathcal{S}$ in Theorem 2 is optimal with respect to the Tang-Fan-Matsufuji bound.

Proof : The proof is straightforward. By substituting $N = p^n - 1$, $M = p^e - 1$, and $\epsilon = 1$ in (11), we have

$$(p^e-1)L-1 \le \frac{p^n-2}{1-1/(p^n-1)}$$

and thus

$$L \le \frac{p^n}{p^e-1}.$$

Since L is an integer, we have

$$L \le \left\lfloor \frac{p^n}{p^e-1} \right\rfloor = \frac{p^n-1}{p^e-1}.$$

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

Example 1: Let $p = 3$, $e = 2$, $n = 4$, and $T = (3^n - 1)/(3^e - 1) = 10$. Let $f(y) = \mathrm{tr}_1^2(y)$ for $y \in F_{3^2}$ and $v(x) = \mathrm{tr}_2^4(x)$ for $x \in F_{3^4}$. Let α be a primitive element in F_{3^4} and $\beta = \alpha^T$. Then the set $\mathcal{S}$ is the 9-ary LCZ sequence set with parameters $(80, 8, 10, 1)$ as follows:

$$\mathcal{S} = \{s_a(x) \mid a \in F_{3^2}^*\}$$

where $s_a(x) = s_a(\alpha^t)$, $0 \le t \le 79$, is given as

$$\begin{aligned}
s_{\beta^0}(\alpha^t) &= s_1(\alpha^t) = p\ \mathrm{tr}_1^4(\alpha^t)\\
&= 60006006606366000360306336060666633306636300030033036330063603603663030333366603363\\
s_{\beta}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^T\alpha^t)\\
&= 836620382327556072676844508658521140254246331064161577305135348870437471228017812\\
s_{\beta^2}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{2T}\alpha^t)\\
&= 263380628687553078373211502352584410851813664031434577605465612270167174882047224\\
s_{\beta^3}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{3T}\alpha^t)\\
&= 863350685651223015313844208328257740524543667034737211602762648810461417558071872\\
s_{\beta^4}(\alpha^t) &= s_2(\alpha^t)\\
&= 2p\ \mathrm{tr}_1^4(\alpha^t)\\
&= 300030033036330063060366303033336660336360006006606366003603063360606666633306636\\
s_{\beta^5}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{5T}\alpha^t)\\
&= 563320652624883042343577805385821170287273661037131844608168675540764741225014512\\
s_{\beta^6}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{6T}\alpha^t)\\
&= 236650325354886045646211802682857710581516337061767844308738312240134147552074272\\
s_{\beta^7}(\alpha^t) &= \mathrm{tr}_1^4(\alpha^t) \boxplus p\ \mathrm{tr}_1^4(\alpha^{7T}\alpha^t)\\
&= 536680358381226018616577205625284470827876334067464211302432375510731714885041542.
\end{aligned}$$

□

4. Conclusions

In this paper, from a p-ary sequence of period $p^n - 1$ with ideal autocorrelation property, we can build an optimal p^2-ary LCZ sequence set with parameters $(p^n - 1, p^e - 1, p^n - 1/p^e - 1, 1)$. This LCZ sequence set can serve as a set of signature sequences with the symbols chosen in the set of p^2-th roots of unity for QS-CDMA systems. This set is optimal in the sense that the set size is maximal given the period of the sequence and the low correlation zone length. Also the set can be viewed as the generalization in terms of alphabet size of the quaternary LCZ sequences set by Kim, Jang, No, and Chung [5].

References

[1] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," IEEE Trans. Veh. Technol., vol.47, no.4, pp.1268–1275, Nov. 1998.

[2] R.A. Scholtz and L.R. Welch, "GMW sequences," IEEE Trans. Inf. Theory, vol.30, no.3, pp.548–553, May 1984.

[3] X.H. Tang and P.Z. Fan, "A class of pseudonoise sequences over GF(p) with low correlation zone," IEEE Trans. Inf. Theory, vol.47, no.4, pp.1644–1649, May 2001.

[4] 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.

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

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

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

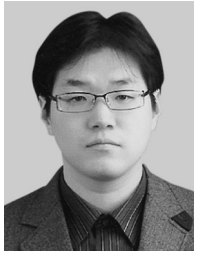
[8] A. Klapper, "d-Form sequence: Families of sequences with low correlation values and large linear spans," IEEE Trans. Inf. Theory, vol.41, no.2, pp.423–431, March 1995.

[9] S.-H. Kim, J.-S. No, H. Chung, and T. Helleseth, "New cyclic relative difference sets constructed from d-homogeneous functions with difference-balance property," IEEE Trans. Inf. Theory, vol.51, no.3, pp.1155–1163, March 2005.

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

[11] J.-W. Jang, J.-S. No, H. Chung, and X. Tang, "New sets of optimal p-ary low correlation zone sequences," Accepted in IEEE Trans. Inf. Theory, 2006.

[12] R. De Gaudenzi, C. Elia, and R. Viola, "Bandlimited quasisynchronous CDMA: A novel satellite access technique for mobile and personal communication systems," IEEE J. Sel. Areas Commun., vol.10, no.2, pp.328–343, Feb. 1992.
[13] T. Helleseth and P.V. Kumar, "Sequences with low correlation," in Handbook of Coding Theory, ed. V.S. Pless and W.C. Huffman, Elservier, Amsterdam, The Netherlands, 1998.
[14] S.-H. Kim and J.-S. No, "New families of binary sequences with low correlation," IEEE Trans. Inf. Theory, vol.49, no.11, pp.3059–3065, Nov. 2003.
[15] J.-S. No, "New cyclic difference sets with Singer parameters constructed from d-homogeneous functions," Des. Codes Cryptogr., vol.33, no.3, pp.199–213, Nov. 2004.
[16] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," Proc. IEEE Int. Symp. Inf. Theory and Its Appl. (ISITA'96), pp.837–840, Victoria, British Columbia, Canada, Sept. 1996.
[17] N. Suehiro, "Approximately synchoronized CDMA system without cochannel using pseudo-periodic sequences," Proc. Int. Symp. Pers. Commun. '93, pp.179–184, Nanjing, China, July 1994.



Ji-Woong Jang was born in 1976. He received the B.S., M.S., and Ph.D. degrees in electronic engineering and computer science from Seoul National University, Seoul, Korea, in 2000, 2002, and 2006, respectively. Since 2006, he is a Senior Engineer at Samsung Electronics, Channel Development Team, Suwon-City, Korea. His area of research interests includes pseudo-noise (PN) sequences, difference sets, cryptography, error correcting codes, and wireless communication systems.

Jong-Seon No received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, Korea, from September 1990 to July 1999. He joined the faculty of the School of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently a Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-times codes, LDPC codes, and wireless communication systems.

Habong Chung received the B.S. degree from Seoul National University, Seoul, in 1981 and the M.S. and the Ph.D. degrees from the University of Southern California, Los Angeles, in 1985 and 1988, respectively. From 1988 to 1991, he was an Assistant Professor in the Department of Electrical and Computer Engineering, the State University of New York at Buffalo. Since 1991, he has been with the School of Electronic and Electrical Engineering, Hongik University, Seoul, where he is a Professor. His research interests include coding theory, combinatorics, and sequence design.