Construction of Optimal p^2-ary Low Correlation Zone Sequences[1]

*Ji-Woong Jang$^{\mathrm{O}}$, *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, 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.

1. Introduction

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. For a prime p, Tang and Fan [2] 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 [3]. Recently, Kim, Jang, No, and Chung proposed quaternary LCZ sequence sets constructed from a binary sequence with ideal autocorrelation [4]. The set of these sequences is optimal with respect to the bound by Tang, Fan, and Matsufuji [5].

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.

2. Preliminaries

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} 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 $m|n$. It is well known that $\mathrm{tr}_m^n(\alpha^t)$ is a p^m-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^2-ary sequences of period p^n-1, which can be regarded as mappings from F_{p^n} to an integer ring $Z_{p^2}=\{0,1,2,\cdots,p^2-1\}$, respectively. We use the notations $\oplus$ and $\ominus$ 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 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

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

where w_{p^2} is a complex p^2-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 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

[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.

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:

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

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 [6] as their constituent sequence.

A d-form function $h(x)$ on F_{p^n} over F_{p^m} [7] 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 [7], a d-form function with difference-balance property plays an important role in designing sequences with ideal autocorrelation. The following lemma is derived in [8].

Lemma 1 [Kim, Chung, and No [8]] 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 [6] constructed unified sequences with ideal autocorrelation from sequences of shorter period with ideal autocorrelation as in the following theorem.

Theorem 2 [No [6]] 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 2 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, then it can serve as $f(y)$ in Theorem 2. 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 2 can be expressed as

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

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 2 can be written as

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

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.

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 3 [Kim, Jang, No, and Chung [4]] 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

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

Then, we have

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

□

Theorem 4 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 2. Define the $p^e - 1$ p^2-ary sequences $s_a(x)$ of period $p^n - 1$ as

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

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 $a, b \in F_{p^e}^*$. The following five separate cases are considered.

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

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

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

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

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

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 3, $R_{a,b}(\delta)$ is rewritten as

$$\begin{aligned} R_{a,b}(\delta) &= \sum_{c \in F_{p^e}^*} \sum_{d \in F_{p^e}^*} M_\delta(cd, d) \\ &\times \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\{f([x_1 cd]^r) \oplus pf([x_1 acd]^r)\} \ominus \{f([x_1 d]^r) \oplus pf([x_1 bd]^r)\}} \\ &+ M_\delta(0,0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^0 \\ &+ \sum_{c \in F_{p^e}^*} M_\delta(c, 0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1 c]^r) \oplus pf([x_1 ac]^r)} \\ &+ \sum_{c \in F_{p^e}^*} M_\delta(0, c) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1 c]^r) \oplus pf([x_1 bc]^r)\}} \\ &= \sum_{c \in F_{p^e}^*} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\{f([x_1 c]^r) \oplus pf([x_1 ac]^r)\} \ominus \{f([x_1]^r) \oplus pf([x_1 b]^r)\}} \\ &\times \sum_{d \in F_{p^e}^*} M_\delta(cd, d) + M_\delta(0,0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^0 \\ &+ \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1]^r) \oplus pf([x_1 a]^r)} \sum_{c \in F_{p^e}^*} M_\delta(c, 0) \\ &+ \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \oplus pf([x_1 b]^r)\}} \sum_{c \in F_{p^e}^*} M_\delta(0, c) \\ &= p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \sum_{c \in F_{p^e}^*} \omega_{p^2}^{\{f(x_1^r [v(\delta x_2)]^r) \ominus f(x_1^r [v(x_2)]^r)\}} \\ &\times \omega_{p^2}^{\{pf(x_1^r a^r [v(\delta x_2)]^r) \ominus pf(x_1^r b^r [v(x_2)]^r)\}} \\ &+ p^{n-2e} - 1 + p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1]^r) \oplus pf([x_1 a]^r)} \\ &+ p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \oplus pf([x_1 b]^r)\}} \\ &= p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \oplus pf([x_1 b]^r)\}} \\ &\times \sum_{c \in F_{p^e}^*} \omega_{p^2}^{f([c]^r) \oplus pf([ac]^r)} + p^{n-2e} - 1 \\ &+ p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1]^r) \oplus pf([x_1 a]^r)} \\ &+ p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-\{f([x_1]^r) \oplus pf([x_1 b]^r)\}}. \end{aligned}$$

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

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

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 $\delta \in F_{p^n} \backslash F_{p^e}$:

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

$$R_{a,b}(\delta) = \sum_{x_2 \in A} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\{f(x_1^r [v(\delta x_2)]^r)\}} \times \omega_{p^2}^{\{f(x_1^r a^r [v(\delta x_2)]^r) \ominus p f(x_1^r [bv(x_2)]^r)\}}$$

$$= \sum_{c \in F_{p^e}^*} \sum_{d \in F_{p^e}^*} M_\delta(cd, d) \times \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{\{f([x_1 cd]^r) \oplus pf([x_1 acd]^r)\} \ominus \{pf([x_1 bd]^r)\}}$$
$$+ M_\delta(0,0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^0$$
$$+ \sum_{c \in F_{p^e}^*} M_\delta(c,0) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1 c]^r) \oplus pf([x_1 ac]^r)}$$
$$+ \sum_{c \in F_{p^e}^*} M_\delta(0,c) \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{-pf([x_1 bc]^r)}$$
$$= p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_p^{-f([bx_1]^r)} \sum_{c \in F_{p^e}^*} \omega_{p^2}^{f([c]^r) \oplus pf([ac]^r)}$$
$$+ p^{n-2e} - 1 + p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_{p^2}^{f([x_1]^r) \oplus pf([x_1 a]^r)}$$
$$+ p^{n-2e} \sum_{x_1 \in F_{p^e}^*} \omega_p^{-f([x_1 b]^r)}.$$

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

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

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 Tang-Fan-Matsufuji bound [5] given as

$$ML - 1 \le \frac{N-1}{1 - \epsilon^2/N} \tag{11}$$

we can check the optimality of p^2-ary LCZ sequence set $\mathcal{S}$ in Theorem 4.

Corollary 5 The p^2-ary LCZ sequence set $\mathcal{S}$ in Theorem 4 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. □

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, pp. 1268–1275, Nov. 1998.

[2] 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.

[3] 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.

[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, Apr. 2005.

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

[6] 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.

[7] 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.

[8] 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. Inform. Theory*, vol. 51, no. 3, pp. 1155–1163, Mar. 2005.