A New Binary Low Correlation Zone Sequences[1]

Ji-Woong Jang O and Jong-Seon No
School of Electrical Engineering and Computer Science
Seoul National University
Email: jsno@snu.ac.kr

Habong Chung
School of Electronic and Electrical Engineering
Hongik University
Email: habchung@hongik.ac.kr

Xiaohu Tang
Institute of Mobile Communications
Southwest Jiaotong University, Chengdu, China
Email: xhutang@ieee.org

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 microcellular or indoor environment, transmission delays are relatively small. Hence, it may be feasible to maintain synchronization within a few chips even in the reverse link. Recently, Gaudenzi, Elia, and Viola proposed the quasi-synchronous CDMA system, which can be applied to the above environment[1]. Long, Zhang, and Hu have shown that the most important property for reducing multiple access interference(MAI) is low correlation property around the origin[5], and they proposed the sequence set that has low correlation value around the origin. 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[5]. For a prime p, Tang and Fan[9] proposed p-ary LCZ sequences by extending the alphabet size of each sequence in Long's work[5]. And they also constructed p-ary LCZ sequences by using interleaved sequences[10]. Kim, Jang, No, and Chung proposed new construction method of quaternary LCZ sequence by using binary sequence of the same period with ideal autocorrelation property[3]. Their method is optimal with respect to the bound by Tang, Fan, and Matsufuji[11]. And they also calculated the correlation distribution of their sequence set constructed from using m-sequence and GMW sequence[3].

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[8]. These new LCZ sequences use Legendre sequences as their column sequences.

[1]This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications.

2. Preliminaries

In this section, we introduce some definitions and notations.

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

Let p be a prime and F_{p^n} be the finite field with p^n elements. Let $s_i(x)$ and $s_j(x)$ 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 $s_i(x)$ and $s_j(x)$ is defined as

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

where ω_p is a primitive p-th root of unity.

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) $\mathrm{tr}_m^n(x^{p^m})=\mathrm{tr}_m^n(x)$, 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}.

Klapper[4] 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 $x\in F_{p^n}$

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

Kim, Jang, No, and Chung[3] derived the following lemma, which can be used in the proof of the following theorem.

Lemma 1 ([3]) Let m, e, and n be positive integers such that $n = em$. Let $q = p^m$ 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

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

Then, we have

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

□

Tang and Fan[10] proposed the construction method of LCZ sequence set by using the interleaved sequence[2] as in the following theorem.

Theorem 1 ([10]) Let e and n be integers such that $e|n$. Let $f(y)$ and $g(y)$ be cyclically distinct binary 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 cross correlation function $R_{f,g}(\delta)$ between $f(h(x))$ and $g(h(x))$ is given as

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

where $I(f) = \sum_{y \in F_{2^m}^*} (-1)^{f(y)}$, $C_{f,g}(\delta) = \sum_{y \in F_{2^m}^*} (-1)^{f(\delta y)+g(y)}$, and $\bar{I}(\cdot)$ denotes complex conjugate of $I(\cdot)$.

Proof: Theorem 1 also can be proven as in the following way.

Case 1) $\delta \in F_{2^m}$

Since $h(x)$ is a 1-form function, $h(\delta x) = \delta h(x)$. Let $N_h(a)$ be the number of $x \in F_{p^n}^*$ such that $h(x) = a$. Then we can rewrite $R_{f,g}(\delta)$ as follows

$$\begin{aligned} R_{f,g}(\delta) &= \sum_{x \in F_{p^n}^*} \omega_p^{f(h(\delta x))-g(h(x))} \\ &= \sum_{x \in F_{p^n}^*} \omega_p^{f(\delta h(x))-g(h(x))} \\ &= \sum_{y \in F_{p^m}} N_h(y) \omega_p^{f(\delta y)-g(y)}. \end{aligned}$$

From the balance property of $h(x)$, $N_h(y)$ has the following values

$$N_h(y) = \begin{cases} p^{n-m}-1, & \text{if } y = 0 \\ p^{n-m}, & \text{otherwise.} \end{cases}$$

Therefore, when $\delta \in F_{p^m}$, $R_{f,g}(\delta)$ is

$$R_{f,g}(\delta) = p^{n-m} C_{f,g}(\delta) + p^{n-m} - 1.$$

Case 2) $\delta \notin F_{p^m}$

Let $T = (p^n-1)/(p^m-1)$. Let $x = x_1 x_2$, where $x_1 \in F_{p^m}$ and $x_2 \in A = \{1, \alpha, \alpha^2, \cdots, \alpha^{T-1}\}$. For $\delta \notin F_{p^m}$, with the replacement of $h(\delta x_2)$ by cd and $h(x_2)$ by d and also from Lemma 1, $R_{f,g}(\delta)$ is rewritten as

$$\begin{aligned} R_{f,g}(\delta) &= \sum_{x \in F_{p^n}^*} \omega_p^{f(h(\delta x))-g(h(x))} \\ &= \sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd,d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 cd)-g(x_1 d)} \\ &\quad + M_\delta(0,0) \sum_{x_1 \in F_{p^m}^*} \omega_p^0 \\ &\quad + \sum_{c \in F_{p^m}^*} M_\delta(c,0) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 c)} \\ &\quad + \sum_{c \in F_{p^m}^*} M_\delta(0,c) \sum_{x_1 \in F_{p^m}^*} \omega_p^{-g(x_1 c)} \\ &= \sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd,d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 cd)-g(x_1 d)} \\ &\quad + p^{n-2m} - 1 + p^{n-2m} I(f) + p^{n-2m} \bar{I}(g). \end{aligned} \tag{3}$$

The first term in the right-hand side of (3) can be rewritten as

$$\begin{aligned} &\sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd,d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 cd)-g(x_1 d)} \\ &= \sum_{c \in F_{p^m}^*} \sum_{d \in F_{p^m}^*} M_\delta(cd,d) \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 c)-g(x_1)} \\ &= p^{n-2m} \sum_{c \in F_{p^m}^*} \sum_{x_1 \in F_{p^m}^*} \omega_p^{f(x_1 c)-g(x_1)} \\ &= p^{n-2m} \left(\sum_{x_1 \in F_{p^m}^*} \omega_p^{-g(x_1)} \right) \left(\sum_{c \in F_{p^m}^*} \omega_p^{f(c)} \right) \\ &= p^{n-2m} I(f) \bar{I}(g). \end{aligned}$$

Therefore, we have

$$R_{f,g}(\delta) = p^{n-2m}(1+I(f))(1+\bar{I}(g)) - 1.$$

□

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

It is clear that $I(f) = -1$ corresponds to the balance property of the column sequence $f(x)$ defined on $F_{p^m}^*$ 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 pairs in the column sequence set have the value -1.

Property 1 Let $\mathcal{S}$ be the set of sequences satisfying the following properties:

i) All sequences in the set are cyclically distinct.

ii) Each sequences in the set has the balance property, that is, the number of zero element is one less than that of each nonzero element in one period of the sequence.

iii) In-phase cross-correlation of each pair of the sequences in the set is always -1.

□

3. New binary LCZ sequence set

In this section, we propose a new binary LCZ sequence set constructed from the binary unified sequence whose column sequences are given by a Legendre sequence.

Let $s(t)$ be a binary sequence from $F_{2^n}^*$ to F_2 and α be a primitive element in F_{2^n}. Then Fourier transform $S(\lambda)$ of the sequence $s(t)$ and its inverse transform are given as

$$\begin{aligned} S(\lambda) &= \sum_{t=0}^{2^n-2} s(t)\alpha^{-\lambda t} \\ s(t) &= \sum_{\lambda=0}^{2^n-2} S(\lambda)\alpha^{\lambda t}. \end{aligned}$$

Legendre sequences of period p for any prime p are defined as

$$s(t) = \begin{cases} 1, & \text{if } t = 0 \bmod p \\ 0, & \text{if } t \text{ is a quadratic residue mod } p \\ 1, & \text{if } t \text{ is a quadratic nonresidue mod } p. \end{cases} \tag{4}$$

And it is well known that $s(t)$, $t = 0, 1, 2, \cdots, p-1$, has ideal autocorrelation if and only if $p \equiv 3 \pmod 4$.

Lemma 2 ([7]) Let e be an integer such that $2^m - 1$ is a prime. Let $s(t)$ be a Legendre sequence defined in (4). Then $s(t)$ can be represented as follows

$$s(t) = \sum_{j \in QR} \alpha^{jt}$$

where α is a primitive element in F_{2^m} and QR is the set of quadratic residues mod $2^m - 1$. □

Theorem 2 Let $e > 3$ be an integer such that $2^m - 1 = p \equiv 3 \pmod 4$ is a prime. Let $s(t)$ be a Legendre sequence of period $2^m - 1$ defined in (4). Then there is no integer pair (a, b) that satisfies the relation

$$s(t) + s(t+a) + s(t+b) = 0, \quad 0 \le a, b \le 2^m - 2. \tag{5}$$

Proof: It is clear that (5) cannot hold when $a = b$. Therefore without loss of generality, we assume $a < b$. Taking Fourier transform of (5), we get the following equation.

$$(1 + \alpha^{\lambda a} + \alpha^{\lambda b})S(\lambda) = 0 \tag{6}$$

where α is a primitive element in F_{2^m}. The above equation implies that for every λ such that

From Lemma 2 and the definition of inverse Fourier transform, we have

$$S(\lambda) = \begin{cases} 1, & \lambda \in QR \\ 0, & \text{otherwise.} \end{cases}$$

If $S(\lambda) \neq 0$, i.e., $\lambda \in QR$, α^λ is always the solution of equation $z^b + z^a + 1 = 0$. It is clear that $\alpha^{-\lambda}$ is the solution of $z^b + z^{b-a} + 1 = 0$, the reciprocal polynomial of $z^b + z^a + 1 = 0$. This means that for each of the quadratic nonresidues λ, α^λ is the solution of $z^b + z^{b-a} + 1 = 0$, since -1 is a quadratic nonresidue. Therefore, we have

$$(z^b + z^a + 1)(z^b + z^{b-a} + 1)(z + 1) \equiv 0 \pmod{z^p - 1}$$

which is equivalent to

$$(z^b + z^a + 1)(z^b + z^{b-a} + 1) = 1 + z + z^2 + \cdots + z^{p-1}.$$

But the equation

$$\begin{aligned} (z^b + z^a + 1)(z^b + z^{b-a} + 1) &= z^{2b} + z^{b+a} + z^{2b-a} \\ &\quad + z^{b-a} + z^b + z^a + 1 \\ &= 1 + z + z^2 + \cdots + z^{p-1} \end{aligned}$$

only holds when $p = 7$ with $(a, b) = (1, 3), (2, 3), (2, 6)$, and $(4, 6)$. That means that if $e > 3$, there is no integer pair (a, b) such that $s(t) + s(t+a) + s(t+b) = 0$. □

Theorem 3 Let $e > 3$ be an integer such that $2^m - 1 = p \equiv 3 \pmod 4$ is a prime. Let $s(t)$ be a Legendre sequence of period $2^m - 1$ defined in (4). Then for nonzero a and $b \neq c$, there is no integer triplet (a, b, c) that satisfies the relation

$$s(t) + s(t+a) + s(t+b) + s(t+c) = 0 \tag{7}$$

except for $(a, 0, a)$ and $(a, a, 0)$.

Proof: It is manifest that (7) holds when $(a, b, c) = (a, 0, a)$ and $(a, b, c) = (a, a, 0)$. Let $a < b < c$ be integers and $S(\lambda)$ be the Fourier transform of $s(t)$. Then by the similar argument in the proof of Theorem 2, we can say that $1 + \alpha^{\lambda a} + \alpha^{\lambda b} + \alpha^{\lambda c} = 0$ for all quadratic

residues λ, and $1+\alpha^{\lambda(c-a)}+\alpha^{\lambda(c-b)}+\alpha^{\lambda c}=0$ for all quadratic nonresidues λ.

Therefore the equation

$$(z^c+z^b+z^a+1)(z^c+z^{c-b}+z^{c-a}+1)\equiv 0 \pmod{z^p-1}$$

holds, since $z=1$ is the common solution of $z^c+z^b+z^a+1=0$ and $z^c+z^{c-b}+z^{c-a}+1=0$. After careful scrutiny, we can deduce that for the integers $a<b<c$, the above equation cannot hold.

□

Using Theorem 1, Theorem 2, and Theorem 3, we can construct binary LCZ sequence with parameters $(2^n-1, 2^{m-1}, (2^n-1)/(2^m-1), 1)$ as in the following theorem.

Theorem 4 Let n and e be integers such that $e|n$ and 2^m-1 is a prime and $T=(2^n-1)/(2^m-1)$. Let α be a primitive element in F_{2^n} and $\beta=\alpha^T$ be a primitive element in F_{2^m}. Let $l(\beta^t)=s(t)$ be the Legendre sequence defined in (4) of period 2^m-1 and the function $h(x)$ from F_{2^n} to F_{2^m} be a 1-form function over F_{2^m} with balance and difference balance property. Then the sequence set $\mathcal{S}$ defined by

$$\mathcal{S}=\{f_i(t) \mid 0\le t\le 2^n-1,\ 0\le i\le 2^{m-1}-1\}$$

where $f_i(t)$ is given as

$$f_i(t)=\begin{cases} l(h(\alpha^t)), & \text{if } i=0\\ l(h(\alpha^t))+l(h(\alpha^{t+Ti})), & \text{if } 1\le i\le 2^{m-1}-1\end{cases}$$

is a $(2^n-1, 2^{m-1}, (2^n-1)/(2^m-1), 1)$ LCZ sequence set.

Proof: From Theorem 2 and Theorem 3, it is clear that all the sequences in $\mathcal{S}$ are cyclically distinct. We should consider the following 4 cases.

Case 1) $i\neq 0$ and $j\neq 0$

It is straight forward that $R_{i,j}(\delta)=2^n-1$ for $i=j$ and $\delta=1$. The correlation $R_{i,j}(\tau)$ between $f_i(t)$ and $f_j(t)$ is given as

$$\begin{aligned} R_{i,j}(\tau) =& \sum_{t=0}^{2^n-2}(-1)^{f_i(t+\tau)+f_j(t)}\\ =& \sum_{t=0}^{2^n-2}(-1)^{\{l(h(\alpha^{t+\tau}))+l(h(\alpha^{t+Ti+\tau}))\}}\\ & \times(-1)^{+\{l(h(\alpha^t))+l(h(\alpha^{t+Tj}))\}}\\ =& \sum_{x\in F_{2^n}^*}(-1)^{\{l(h(\delta x))+l(h(\delta a x))\}}\\ & \times(-1)^{\{l(h(x))+l(h(bx))\}} \end{aligned} \quad (8)$$

where $a=\alpha^{Ti}$, $b=\alpha^{Tj}$, and $\delta=\alpha^\tau$.

From Theorem 1 and (8), $R_{i,j}(\tau)=R_{a,b}(\delta)$ can be rewritten as

$$R_{i,j}(\tau)=\begin{cases} 2^{n-2m}(I(g_i)+1)(I(g_j)+1)-1, & \text{if } \delta\notin F_{2^m}\\ 2^{n-m}C_{g_i,g_j}(\delta)+2^{n-m}-1, & \text{if } \delta\in F_{2^m}\end{cases}$$

where $g_i(y)=l(y)+l(\alpha^{Ti}y)$. Since the Legendre sequence has difference-balance property, it is easy to see that $I(g_i)=-1$ for any i. It is also clear that $C_{i,j}(1)=-1$ for any i and j. Therefore when $i\neq 0$ and $j\neq 0$, f_i and f_j has the low correlation zone $[1-T, T-1]$.

Case 2) $i=0$ and $j\neq 0$

In this case, the correlation $R_{i,0}(\tau)$ between $f_i(t)$ and $f_0(t)$ is given as

$$\begin{aligned} R_{i,0}(\tau) &= \sum_{t=0}^{2^n-2}(-1)^{f_i(t+\tau)+f_0(t)}\\ &= \sum_{t=0}^{2^n-2}(-1)^{\{l(h(\alpha^{t+\tau}))+l(h(\alpha^{t+Ti+\tau}))\}+\{l(h(\alpha^t))\}}\\ &= \sum_{x\in F_{2^n}^*}(-1)^{\{l(h(\delta x))+l(h(\delta a x))\}+\{l(h(x))\}}. \end{aligned} \quad (9)$$

From Theorem 1 and (8), $R_{i,0}(\tau)=R_{a,1}(\delta)$ can be rewritten as

$$R_{i,0}(\tau)=\begin{cases} 2^{n-2m}(I(g_i)+1)(I(g_0)+1)-1, & \text{if } \delta\notin F_{2^m}\\ 2^{n-m}C_{g_i,g_0}(\delta)+2^{n-m}-1, & \text{if } \delta\in F_{2^m}\end{cases}$$

where $g_0(y)=l(y)$. Since the Legendre sequence has balance and difference-balance property, it is easy to see that $I(g_i)=-1$ for any i and $I(g_0)=-1$. It also clear that $C_{i,0}(1)=-1$ for any i. Therefore when $i\neq 0$ and $j=0$, f_i and f_j has low correlation zone $[1-T, T-1]$.

Case 3) $i\neq 0$ and $j=0$

In a similar way to case 2), it is manifest that $R_{0,j}(\tau)=R_{1,b}(\delta)$ is given as

$$R_{0,j}(\tau)=\begin{cases} 2^{n-2m}(I(g_0)+1)(I(g_j)+1)-1, & \text{if } \delta\notin F_{2^m}\\ 2^{n-m}C_{g_0,g_j}(\delta)+2^{n-m}-1, & \text{if } \delta\in F_{2^m}.\end{cases}$$

From the above equation, it is straightforward that f_i and f_j has low correlation zone $[1-T, T-1]$ for $i=0$ and $j\neq 0$.

Case 4) $i=j=0$

It is clear that $R_{0,0}(\delta)=2^n-1$. And similarly to case 1), $R_{0,0}(\tau)=R_{1,1}(\delta)$ is given as

$$R_{0,0}(\tau)=\begin{cases} 2^{n-2m}(I(g_0)+1)(I(g_0)+1)-1, & \text{if } \delta\notin F_{2^m}\\ 2^{n-m}C_{g_0,g_0}(\delta)+2^{n-m}-1, & \text{if } \delta\in F_{2^m}.\end{cases}$$

Again from the balance and difference-balance property of the Legendre sequence, we have $R_{1,1}(\delta)=-1$ for $\delta\in\{\alpha^{1-T}, \alpha^{2-T}, \cdots, \alpha^{-1}, \alpha, \alpha^2, \cdots, \alpha^{T-2}, \alpha^{T-1}\}$.

From the above 4 cases, $\mathcal{S}$ is the LCZ sequence set with parameters $(2^n-1, 2^{m-1}, (2^n-1)/(2^m-1), 1)$.□

No, Lee, Chung, Song, and Yang found the trace representation of Legendre sequence as following theorem.

Theorem 5 ([7]) Let $p = 2^m - 1$ be a prime for some integer $m \geq 3$ and u be a primitive element in Z_p, the set of integers mod p. Let α be a primitive element of F_{2^m} such that

$$\sum_{i=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m(\alpha^{u^{2i}}) = 0.$$

Then the sequence $s(t)$ for $t = 0, 1, 2, \cdots, p-1$ of period p given by

$$s(t) = \sum_{i=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m(\alpha^{u^{2i}t})$$

is the Legendre sequence given in (4).

□

Using the above theorem, we can represent the new binary LCZ sequence as in the closed form in the following corollary.

Corollary 1 Let m and n be integers such that $e|n$ and $2^m - 1$ be a prime. Let α be the primitive element in F_{2^n} and $h(y) = \mathrm{tr}_m^n(y)$. Then the sequence $f_i(t)$ defined in Theorem 4 can be represent as

$$f_i(t) = \begin{cases} \sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^t)]^{u^{2j}}), & i = 0 \\ \sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^t)]^{u^{2j}}) \\ + \sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^{t+i})]^{u^{2j}}), & 1 \leq i \leq 2^{m-1} - 1 \end{cases}$$

where u is defined in Theorem 5 and $p = 2^m - 1$.

□

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] S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *IEEE Tras. on Inform. Theory*, vol. 51, no. 3, pp. 1155-1163, Apr. 2005.

[4] 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.

[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] Jong-Seon No, "p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation property," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2540-2546, September 2002.

[7] 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. on Inform. Theory,* vol. 42, no. 6, pp. 2254-2255, Nov. 1996.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.