# New Quaternary Low Correlation Zone Sequences

Sang-Hyo Kim
Wireless Device Solution Team
Telecomm. R&D Center
Samsung Electronics
Suwon, Korea
sanghyo7.kim@samsung.com

Ji-Woong Jang, Kyoung-Young Song
School of EE and CS
Seoul National University
Seoul, Korea
{stasera,sky6174}@ccl.snu.ac.kr

Jong-Seon No
School of EE and CS
Seoul National University
Seoul, Korea
jsno@snu.ac.kr

Habong Chung
School of EEE
Hongik University
Seoul, Korea
habchung@hongik.ac.kr

*Abstract*— **In this paper, given a composite integer $n$, we propose a method of constructing quaternary low correlation zone(LCZ) sequences of period $2^n-1$ from binary sequences of the same length with ideal autocorrelation. These new sequences are optimal with respect to the bound by Tang, Fan, and Matsufuji. The correlation distributions of these new quaternary LCZ sequences constructed from m-sequences and GMW sequences are derived.**

## I. Introduction

In a microcellular communication environment such as wireless local area networks(LAN), where the cell size is very small, transmission delay is relatively small and thus it is possible to maintain the time delay in reverse link within a few chips. In such a system as the quasi-synchronous code-division multiple-access(QS-CDMA) system proposed by Gaudenzi, Elia, and Vilola[1], multiple chip time delay among different users is allowed, which gives the more flexibility in designing the wireless communication system.

In the design of a sequence set for QS-CDMA system, what matters most is to have low correlation zone around origin rather than to minimize the overall maximum nontrivial correlation value[6]. In fact, low correlation zone(LCZ) sequences with smaller correlation magnitude within the zone show better performance than other well-known sequence sets with optimal correlation property[6]. 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 $\epsilon$ within the range $-L < \tau < L$, of the offset $\tau$, then $\mathcal{S}$ is called an $(N, M, L, \epsilon)$ LCZ sequence set.

In this paper, given a composite integer $n$, we propose a method of constructing quaternary LCZ sequences of period $2^n-1$ from binary sequences of the same length with ideal autocorrelation. These new sequences are optimal with respect to the bound by Tang, Fan, and Matsufuji[9]. The correlation distributions of these new quaternary LCZ sequences constructed from m-sequences and GMW sequences are derived.

## II. Preliminaries

In this section, we introduce some definitions and notations. In this paper, we only deal with binary and quaternary sequences of period $2^n-1$, which can be regarded as mappings from $F_{2^n}$ to $F_2$ and to the integer ring $Z_4 = \{0,1,2,3\}$, respectively. We use the notations $\boxplus$ and $\boxminus$ for the addition and the subtraction in $Z_4$, only if we think it is necessary.

Let $F_{2^n}^* = F_{2^n} \setminus \{0\}$ and $s(x)$ be a mapping from $F_{2^n}$ to $F_2$ or $Z_4$. If we restrict the mapping $s(x)$ to $F_{2^n}^*$ and replace $x$ by $\alpha^t$, then we can obtain a sequence $s(\alpha^t)$, $0 \le t \le 2^n-2$, of period $2^n-1$. Hence, for convenience, we will use the expression 'a binary or quaternary sequence $s(\alpha^t)$ of period $2^n-1$' interchangeably with 'a mapping $s(x)$ from $F_{2^n}$ to $F_2$ or $Z_4$'.

Let $f(x)$ be a mapping from $F_{2^n}$ onto $F_{2^e}$, where $e|n$. The function $f(x)$ is said to be *balanced* if each nonzero element of $F_{2^e}$ appears $2^{n-e}$ times and zero element $2^{n-e}-1$ times in the list $\{f(x)|x \in F_{2^n}^*\}$. A function $f(x)$ is said to be *difference-balanced* if $f(\delta x) - f(x)$ is balanced for any $\delta \in F_{2^n} \setminus \{0,1\}$.

It is not difficult to see that a quaternary sequence can be decomposed into two constituent binary sequences. Let $v_1$ and $v_2$ be variables over $Z_2$, i.e., Boolean variables. Then a variable $v$ over $Z_4$ can be expressed as

$$v = v_1 \boxplus 2v_2. \tag{1}$$

Let us use the notation $v = (v_2, v_1)$ to alternatively represent (1). Let $\phi(\cdot)$ and $\psi(\cdot)$ be the maps defined by

$$\phi(v) = v_1, \quad \psi(v) = v_2.$$

Applying Karnaugh map, $\phi(v-w)$ and $\psi(v-w)$ are expressed as

$$\begin{aligned} \phi(v-w) &= v_1 + w_1 \\ \psi(v-w) &= v_1 w_1 + w_1 + w_2 + v_2. \end{aligned}$$

Let $v(x)$, $w(x)$, and $d(x)$ be quaternary sequences given as

$$v(x) = v_1(x) \boxplus 2v_2(x), \quad w(x) = w_1(x) \boxplus 2w_2(x)$$

and

$$d(x) = v(x) - w(x)$$

where $x \in F_{2^n}^*$. Then, the mappings $\phi$ and $\psi$ of the quaternary sequence $d(x)$ are given by

$$\phi(d(x)) = v_1(x) + w_1(x) \tag{2}$$

$$\psi(d(x)) = v_1(x)w_1(x) + w_1(x) + w_2(x) + v_2(x). \tag{3}$$

## III. Quaternary LCZ sequences constructed from m-sequences

In this section, we construct a set of quaternary LCZ sequences using an m-sequence as their constituent sequences. The following lemma is useful in the computation of the correlation of these quaternary LCZ sequences.

*Lemma 1:* Let $s(x)$ be a function from $F_{2^n}$ to $Z_4$, where $s(0) = 0$. We define two Boolean constituent functions of $s(x)$ as

$$\phi_s(x) = \phi(s(x)), \quad \psi_s(x) = \psi(s(x))$$

and their modulo-2 sum as

$$\mu_s(x) = \phi_s(x) + \psi_s(x). \tag{4}$$

Let $N_f(c)$ denote the number of occurrences of $f(x) = c$ as $x$ varies over $F_{2^n}$. Then, we have

$$\sum_{x \in F_{2^n}} \omega_4^{s(x)} = (N_{\psi_s}(0) - N_{\mu_s}(1)) + j(N_{\mu_s}(1) - N_{\psi_s}(1)). \tag{5}$$

□

*Corollary 2:* Let $s(x)$ be a function from $F_{2^n}$ to $Z_4$. Then,

$$\sum_{x \in F_{2^n}} \omega_4^{s(x)} = 0$$

if and only if the functions $\psi_s(x)$ and $\mu_s(x)$ are balanced.

□

Let $f(x)$ be a function from $F_{2^n}$ to $F_2$. We can use $f(x)$ as the constituent sequence of a quaternary sequence $q(x)$ as

$$q(x) = f(x) \boxplus 2f(ax)$$

where $a \in F_{2^n} \setminus F_2$. Most of sequences in this paper are constructed in this manner. We can derive the crosscorrelation values between two quaternary sequences constructed from an m-sequence.

*Theorem 3:* Let $m_a(x)$ and $m_b(x)$ be two quaternary sequences defined by the functions

$$\begin{aligned} m_a(x) &= \mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(ax) \\ m_b(x) &= \mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(bx) \end{aligned}$$

where $a, b \in F_{2^n} \setminus F_2$. Then, their correlation values are given as

$$R_{a,b}(\delta) = \begin{cases} 2^n - 1, & a = b \text{ and } \delta = 1 \\ -1 + 2^{n-1}, & a \neq b \text{ and } \delta = \frac{b}{a} \text{ or } \frac{b+1}{a+1} \\ -1 + j2^{n-1}, & \delta = \frac{b+1}{a} \\ -1 - j2^{n-1}, & \delta = \frac{b}{a+1} \\ -1, & \text{otherwise} \end{cases}$$

where $j = \sqrt{-1}$.

*Proof :* Let $d(x) = m_a(\delta x) - m_b(x)$. The crosscorrelation function between two sequences $m_a(x)$ and $m_b(x)$ is given by

$$R_{a,b}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{d(x)} = -1 + \sum_{x \in F_{2^n}} \omega_4^{d(x)}. \tag{6}$$

From (2) and (3), we have

$$\begin{aligned} \phi_d(x) = \phi(d(x)) &= \mathrm{tr}_1^n(\delta x) + \mathrm{tr}_1^n(x) \\ \psi_d(x) = \psi(d(x)) &= \mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((\delta a + 1 + b)x) \\ \mu_d(x) = \mu(d(x)) &= \mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((\delta(a+1) + b)x). \end{aligned}$$

Define

$$S_{\psi_d}(\delta) = N_{\psi_d}(0) - N_{\psi_d}(1) \tag{7}$$

$$S_{\mu_d}(\delta) = N_{\mu_d}(0) - N_{\mu_d}(1). \tag{8}$$

In order to derive $R_{a,b}(\delta)$, we have to compute $N_{\psi_d}(0)$, $N_{\psi_d}(1)$, and $N_{\mu_d}(1)$ from $S_{\psi_d}(\delta)$ and $S_{\mu_d}(\delta)$.

**Case 1)** $a \neq b$ :

For $\delta = 1$, we have

$$S_{\psi_d}(1) = S_{\mu_d}(1) = \sum_{x \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((b+1+a)x)}.$$

From the linearity and balance property of $\mathrm{tr}_1^n(x)$, we have

$$S_{\psi_d}(1) = S_{\mu_d}(1) = 0.$$

From Corollary 2, we have

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

Next we consider the case of $\delta \in F_{2^n} \setminus F_2$. For a Boolean function $k(x)$ on $F_{2^n}$, we can define a trace transform $K(\lambda)$ given by

$$K(\lambda) = \sum_{x \in F_{2^n}} (-1)^{k(x) + \mathrm{tr}_1^n(\lambda x)}.$$

It is obvious that $S_{\psi_d}(\delta)$ and $S_{\mu_d}(\delta)$ in (7) and (8) are the trace transform values of the quadratic Boolean function

$$k(x) = \mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x)$$

evaluated at $\lambda = \delta a + 1 + b$ and $\lambda = \delta(a+1) + b$, respectively.

The rank of the quadratic Boolean function $k(x)$ gives its distribution of trace transform values (see Theorem 6.2 of [3]). Now we have to examine the bilinear form of $k(x)$ to compute the rank of the quadratic Boolean function $k(x)$ [4]. The bilinear form of $k(x)$ is given by

$$\begin{aligned} B_k(x, y) &= k(x) + k(y) + k(x + y) \\ &= \mathrm{tr}_1^n(\delta y)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(y) \\ &= \mathrm{tr}_1^n(x[\mathrm{tr}_1^n(\delta y) + \delta \mathrm{tr}_1^n(y)]). \end{aligned}$$

The number of $y$ which satisfies $B_k(x, y) = 0$ for all $x$ is equal to that of the solutions to the equation

$$\mathrm{tr}_1^n(\delta y) + \delta \mathrm{tr}_1^n(y) = 0.$$

Since $\delta \in F_{2^n} \setminus F_2$, the number of solutions is equal to the number of $y \in F_{2^n}$ satisfying

$$\mathrm{tr}_1^n(\delta y) = 0 \quad \text{and} \quad \mathrm{tr}_1^n(y) = 0, \tag{9}$$

which is obviously $2^{n-2}$ derived from the difference-balance property of the trace function. Thus the rank of the quadratic form is $n - (n-2) = 2$.

From Theorem 6.2 of [3], we have

$$K(\lambda)=\begin{cases}0, & 2^n-4 \text{ times}\\ 2^{n-1}, & 3 \text{ times}\\ -2^{n-1}, & \text{once.}\end{cases} \tag{10}$$

It is not difficult to derive the values of $\lambda$ which yield nonzero $K(\lambda)$. For $\lambda=0$,

$$K(0)=\sum_{x\in F_{2^n}}(-1)^{\mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x)}=2^{n-1}$$

because $(\mathrm{tr}_1^n(\delta x),\mathrm{tr}_1^n(x))=(1,1)$ occurs $2^{n-2}$ times as $x$ varies over $F_{2^n}$. In a similar way, we have

$$K(\lambda)=\begin{cases}2^{n-1}, & \lambda=0,1,\delta\\ -2^{n-1}, & \lambda=1+\delta\\ 0, & \text{otherwise.}\end{cases} \tag{11}$$

Since $S_\psi(\delta)$ and $S_\mu(\delta)$ are $K(\lambda)$ evaluated at $\lambda=\delta a+1+b$ and $\delta(a+1)+b$, respectively, (11) can be rewritten as

$$S_{\psi_d}(\delta)=\begin{cases}2^{n-1}, & \delta=\frac{b+1}{a},\frac{b}{a},\frac{b+1}{a+1}\\ -2^{n-1}, & \delta=\frac{b}{a+1}\\ 0, & \text{otherwise}\end{cases} \tag{12}$$

and

$$S_{\mu_d}(\delta)=\begin{cases}2^{n-1}, & \delta=\frac{b}{a+1},\frac{b+1}{a+1},\frac{b}{a}\\ -2^{n-1}, & \delta=\frac{b+1}{a}\\ 0, & \text{otherwise}\end{cases} \tag{13}$$

for $\delta\in F_{2^n}^*$.

Finally from (7), (8), (12), and (13), we have

$$R_{a,b}(\delta)=\begin{cases}-1+j2^{n-1}, & \delta=\frac{b+1}{a}\\ -1+2^{n-1}, & \delta=\frac{b}{a},\ \frac{b+1}{a+1}\\ -1-j2^{n-1}, & \delta=\frac{b}{a+1}\\ -1, & \text{otherwise.}\end{cases}$$

**Case 2)** $a=b$ :

When $\delta=1$, it is straightforward that $d(x)=0$ and $R_{a,a}(1)=2^n-1$. For $\delta\in F_{2^n}\setminus F_2$, we have

$$S_{\psi_d}(\delta)=\begin{cases}2^{n-1}, & \delta=\frac{a+1}{a}\\ -2^{n-1}, & \delta=\frac{a}{a+1}\\ 0, & \text{otherwise}\end{cases} \tag{14}$$

and

$$S_{\mu_d}(\delta)=\begin{cases}2^{n-1}, & \delta=\frac{a}{a+1}\\ -2^{n-1}, & \delta=\frac{a+1}{a}\\ 0, & \text{otherwise.}\end{cases} \tag{15}$$

Thus the correlation distribution is given by

$$R_{a,a}(\delta)=\begin{cases}2^n-1, & \delta=1\\ -1+j2^{n-1}, & \delta=\frac{a+1}{a}\\ -1-j2^{n-1}, & \delta=\frac{a}{a+1}\\ -1, & \text{otherwise}\end{cases}$$

for $\delta\in F_{2^n}^*$. □

Theorem 3 tells us that for all but 4 values of $\delta$, the crosscorrelation function $R_{a,b}(\delta)$ takes the value $-1$, which motivates us to construct a set of quaternary LCZ sequences as in the following theorem.

*Theorem 4:* Let $n$ and $e$ be positive integers such that $e|n$. Let $\beta$ be a primitive element in $F_{2^e}$ and $T=(2^n-1)/(2^e-1)$. Let $\mathcal{M}=\{m_i(x)|0\le i\le 2^e-2,\ x\in F_{2^n}^*\}$ be the set of quaternary sequences defined by the functions

$$\begin{aligned}m_0(x)&=2\mathrm{tr}_1^n(x)\\ m_i(x)&=\mathrm{tr}_1^n(x)\boxplus 2\mathrm{tr}_1^n(\beta^i x),\quad \text{for } 1\le i\le 2^e-2.\end{aligned} \tag{16}$$

Then, the set $\mathcal{M}$ is a $(2^n-1,2^e-1,T,1)$ LCZ sequence set and has the following correlation distribution:

$$\begin{aligned}R_{i,k}(\delta) &= \sum_{x\in F_{2^n}^*} w_4^{m_i(\delta x)-m_k(x)} \\ &= \begin{cases}2^n-1, & 2^e-1 \text{ times}\\ -1+j2^{n-1}, & (2^e-2)^2 \text{ times}\\ -1-j2^{n-1}, & (2^e-2)^2 \text{ times}\\ -1+2^{n-1}, & 2(2^e-2)(2^e-3) \text{ times}\\ 2^{n-1}-1+j2^{n-1}, & 2(2^e-2) \text{ times}\\ 2^{n-1}-1-j2^{n-1}, & 2(2^e-2) \text{ times}\\ -1, & \text{otherwise}\end{cases}\end{aligned} \tag{17}$$

as $\delta$ varies over $F_{2^n}^*$ and $0\le i,k\le 2^e-2$.

*Proof :* Set $\delta=\alpha^\tau$. Let $d(x)=m_i(\delta x)-m_k(x)$. We consider the following five cases.

**Case 1)** $i=k=0$ (once):

In this case, $R_{0,0}(\delta)$ can be rewritten as

$$R_{0,0}(\delta)=\sum_{x\in F_{2^n}^*} w_4^{2\mathrm{tr}_1^n((\delta+1)x)}=\begin{cases}2^n-1, & \text{once for } \delta=1\\ -1, & 2^n-2 \text{ times}\\ & \text{for } \delta\in F_{2^n}\setminus F_2.\end{cases}$$

**Case 2)** $i=k\neq 0$ ($2^e-2$ times):

Let $a=\beta^i=\beta^k$. From Theorem 3, the correlation function is given as

$$R_{i,i}(\delta)=\begin{cases}2^n-1, & \text{once for } \delta=1\\ -1+j2^{n-1}, & \text{once for } \delta=\frac{a+1}{a}\\ -1-j2^{n-1}, & \text{once for } \delta=\frac{a}{a+1}\\ -1, & 2^n-4 \text{ times}\\ & \text{for } \delta\neq 1,\ \frac{a+1}{a},\ \frac{a}{a+1}\end{cases}$$

for $\delta\in F_{2^n}^*$.

**Case 3)** $i\neq 0$ and $k=0$ ($2^e-1$ times) :

Set $a=\beta^i$. Then $d(x)$ is given by $d(x)=\{\mathrm{tr}_1^n(\delta x)\boxplus 2\mathrm{tr}_1^n(a\delta x)\}-2\mathrm{tr}_1^n(x)$. Thus $R_{i,0}(\delta)$ is written as

$$R_{i,0}(\delta)=\sum_{x\in F_{2^n}^*}\omega_4^{\mathrm{tr}_1^n(\delta x)\boxplus 2(\mathrm{tr}_1^n(a\delta x)+\mathrm{tr}_1^n(x))}.$$

It is clear that $N_{\psi_d}(0)=2^n$ if $\delta=1/a$ and $2^{n-1}$, otherwise. And $N_{\mu_d}(0)=2^n$ if $\delta=1/(a+1)$ and $2^{n-1}$, otherwise. Using

Lemma 1, we have

$$R_{i,0}(\delta)=\begin{cases}2^{n-1}-1+j2^{n-1}, & \text{once for } \delta=\frac{1}{a}\\ 2^{n-1}-1-j2^{n-1}, & \text{once for } \delta=\frac{1}{a+1}\\ -1, & 2^n-3 \text{ times}\\ & \text{for } \delta\neq\frac{1}{a},\frac{1}{a+1}.\end{cases}$$

**Case 4)** $i=0$ and $k\neq 0$ ($2^e-1$ times) :

Set $b=\beta^k$. Similarly to Case 3, we have

$$R_{0,k}(\delta)=\begin{cases}2^{n-1}-1+j2^{n-1}, & \text{once for } \delta=b\\ 2^{n-1}-1-j2^{n-1}, & \text{once for } \delta=b+1\\ -1, & 2^n-3 \text{ times}\\ & \text{for } \delta\neq b,b+1.\end{cases}$$

**Case 5)** $i\neq k$, $i\neq 0$, and $k\neq 0$ ($(2^e-1)(2^e-2)$ times ):

Let $a=\beta^i$ and $b=\beta^k$. The crosscorrelation function between the two sequences $m_i(x)$ and $m_k(x)$ is given by

$$R_{i,k}(\delta)=\sum_{x\in F_{2^n}^*}\omega_4^{(\mathrm{tr}_1^n(x\delta)\boxplus 2\mathrm{tr}_1^n(ax\delta))-(\mathrm{tr}_1^n(x)\boxplus 2\mathrm{tr}_1^n(bx))}.$$

From Theorem 3, we have

$$R_{i,k}(\delta)=\begin{cases}-1+j2^{n-1}, & \text{once for } \delta=\frac{b+1}{a}\\ -1+2^{n-1}, & \text{twice for } \delta=\frac{b}{a} \text{ or } \frac{b+1}{a+1}\\ -1-j2^{n-1}, & \text{once for } \delta=\frac{b}{a+1}\\ -1, & 2^n-5 \text{ times}\\ & \text{for } \delta\neq\frac{b+1}{a},\ \frac{b}{a},\ \frac{b+1}{a+1},\ \frac{b}{a+1}.\end{cases}$$

Given any pair of sequences in the set $\mathcal{M}$, the correlation functions have the low correlation zone $(-T,T)$. We can derive (17) by combining the above 5 cases. □

*Remark 5:* The set $\mathcal{M}$ is optimal with respect to the Tang-Fan-Matsufuji bound[9]. □

## IV. Quaternary LCZ sequences constructed from GMW sequences and extended sequences

The quaternary LCZ sequences in the set $\mathcal{M}$ are constructed with m-sequences as their constituent sequences. In this section, we apply the same method to construct the set $\mathcal{G}$ of quaternary LCZ sequences from GMW sequences. It has the same correlation property and low correlation zone as those of $\mathcal{M}$.

Klapper[5] 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 $x\in F_{p^n}$

$$H(yx)=y^dH(x). \tag{18}$$

*Lemma 6:* Let $m$, $e$, and $n$ be positive integers such that $n=em$. Let $q=2^e$ and $A=\{1,\alpha,\cdots,\alpha^{T-1}\}$, where $\alpha$ is a primitive element in $F_{2^n}$ 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

$$v(\delta x_2)=a \ \text{ and } \ v(x_2)=b, \quad a,b\in F_q. \tag{19}$$

Then, we have

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

□

*Theorem 7:* Let $n$ and $e$ be positive integers such that $e|n$ and $T=(2^n-1)/(2^e-1)$. Let $r$ be an integer such that $\gcd(r,2^e-1)=1$ and $1\le r\le 2^e-2$. Let $g(x)$ be the GMW sequence defined by

$$g(x)=\mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^r).$$

Let us define the family $\mathcal{G}=\{g_i(x)|0\le i\le 2^e-2,\ x\in F_{2^n}^*\}$ of quaternary sequences defined by

$$\begin{aligned}g_0(x) &= 2\mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^r)\\ g_i(x) &= \mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^r)\boxplus 2\mathrm{tr}_1^e([\beta^i\mathrm{tr}_e^n(x)]^r), \qquad (20)\\ &\quad 1\le i\le 2^e-2\end{aligned}$$

where $\beta$ is a primitive element in $F_{2^e}$. Then, $\mathcal{G}$ has the same correlation distribution as that of $\mathcal{M}$ and is a $(2^n-1,2^e-1,T,1)$ LCZ sequence set.

*Proof :* There is one-to-one correspondence between $\mathcal{M}$ and $\mathcal{G}$ so that the correlation distribution of any given pair of sequences in $\mathcal{G}$ is identical to that of corresponding two sequences in $\mathcal{M}$. But we omit the proof for space limitation. □

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.

*Lemma 8:* Let $f(x)$ be a function from $F_{2^e}$ to $F_2$ with balance and difference-balance property and $f(0)=0$. For $a,b\in F_{2^e}\setminus F_2$, define two quaternary sequences $u_a(x)$ and $u_b(x)$ as

$$\begin{aligned}u_a(x) &= f(x)\boxplus 2f(ax)\\ u_b(x) &= f(x)\boxplus 2f(bx)\end{aligned}$$

and let $d(x)=u_a(\delta x)-u_b(x)$. Then

$$S_{\psi_d}=\sum_{\delta\in F_{2^e}^*}\sum_{x\in F_{2^e}^*}(-1)^{\psi_d(x)}=1$$

and

$$S_{\mu_d}=\sum_{\delta\in F_{2^e}^*}\sum_{x\in F_{2^e}^*}(-1)^{\mu_d(x)}=1.$$

□

Using the extended sequences by No, Yang, Chung, and Song[7], we can construct LCZ sequences as in the following theorem.

*Theorem 9:* Let $n$ and $e$ be positive integers such that $e|n$. Let $f(x)$ be the function from $F_{2^e}$ to $F_2$ with difference-balance property such that $f(0)=0$. Let $r$ be an integer

such that $\gcd(r, 2^e-1) = 1$ and $1 \le r \le 2^e-2$. Let $\beta$ be a primitive element in $F_{2^e}$. Let $\mathcal{H}$ be the set of $2^e-1$ quaternary sequences defined by the functions

$$\begin{aligned} h_0(x) &= 2f([\mathrm{tr}_e^n(x)]^r) \\ h_i(x) &= f([\mathrm{tr}_e^n(x)]^r) \boxplus 2f([\beta^i \mathrm{tr}_e^n(x)]^r), \quad 1 \le i \le 2^e-2. \end{aligned}$$

Then, $\mathcal{H}$ is a $(2^n-1, 2^e-1, (2^n-1)/(2^e-1), 1)$ LCZ sequence set.

*Proof :* Consider two sequences in $\mathcal{H}$ given by

$$\begin{aligned} h_i(x) &= f([\mathrm{tr}_e^n(x)]^r) \boxplus 2f(a^r[\mathrm{tr}_e^n(x)]^r) \\ h_k(x) &= f([\mathrm{tr}_e^n(x)]^r) \boxplus 2f(b^r[\mathrm{tr}_e^n(x)]^r) \end{aligned}$$

where $a^r = \beta^i$ and $b^r = \beta^k$ for nonzero $i$ and $k$. 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)** $i \ne k$ :

Then $R_{i,k}(\delta)$ is given by

$$\begin{aligned} R_{i,k}(\delta) &= \sum_{x_2 \in A} \sum_{x_1 \in F_{2^e}^*} \omega_4^{\left\{f(x_1^r[\mathrm{tr}_e^n(\delta x_2)]^r) \boxplus 2f(x_1^r a^r[\mathrm{tr}_e^n(\delta x_2)]^r)\right\}} \\ &\qquad \times \omega_4^{-\left\{f(x_1^r[\mathrm{tr}_e^n(x_2)]^r) \boxplus 2f(x_1^r b^r[\mathrm{tr}_e^n(x_2)]^r)\right\}}. \end{aligned}$$

For $\delta \notin F_{2^e}$, 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 6, $R_{i,k}(\delta)$ is rewritten as

$$\begin{aligned} R_{i,k}(\delta) &= \sum_{d \in F_{2^e}^*} M_\delta(cd, d) \sum_{c \in F_{2^e}^*} \sum_{x_1 \in F_{2^e}^*} \omega_4^{\{f([x_1 cd]^r) \boxplus 2f([x_1 acd]^r)\}} \\ &\qquad \times \omega_4^{-\{f([x_1 d]^r) \boxplus 2f([x_1 bd]^r)\}} \\ &\quad + M_\delta(0,0) \sum_{x_1 \in F_{2^e}^*} \omega_4^0 \\ &\quad + \sum_{c \in F_{2^e}^*} M_\delta(c, 0) \sum_{x_1 \in F_{2^e}^*} \omega_4^{\{f([x_1 c]^r) \boxplus 2f([x_1 ac]^r)\}} \\ &\quad + \sum_{c \in F_{2^e}^*} M_\delta(0, c) \sum_{x_1 \in F_{2^e}^*} \omega_4^{-\{f([x_1 c]^r) \boxplus 2f([x_1 bc]^r)\}}. \end{aligned}$$

From Lemma 1 and Lemma 8, $R_{i,k}(\delta)$ can be computed as

$$R_{i,k}(\delta) = 2^{n-2e} + 2^{n-2e} - 1 + 2 \cdot 2^{n-2e}(-1) = -1.$$

For $\delta = 1$, we have

$$\begin{aligned} R_{i,k}(1) &= \sum_{x \in F_{2^n}^*} \omega_4^{(f([\mathrm{tr}_e^n(x)]^r) \boxplus 2f(a^r[\mathrm{tr}_e^n(x)]^r))} \\ &\qquad \times \omega_4^{-(f([\mathrm{tr}_e^n(x)]^r) \boxplus 2f(b^r[\mathrm{tr}_e^n(x)]^r))} \\ &= -1 \end{aligned}$$

from the difference-balance property of $f(x)$.

**Case 2)** $i = k$ :

Obviously, $R_{i,i}(1) = 2^n - 1$. When $\delta \notin F_{2^e}$, by the similar way to Case 1), the correlation function is given as

$$R_{i,i}(\delta) = 2^{n-2e} + 2^{n-2e} - 1 + 2 \cdot 2^{n-2e}(-1) = -1.$$

The remaining part is the case when either of the two sequences is $h_0(x)$. In this case, it is easy to show that $R_{i,0}(\delta) = R_{0,i}(\delta) = -1$ for $\delta \in F_{2^e} \setminus F_2$ and $R_{0,0}(\delta) = -1$ for $\delta \ne 1$.

Thus the correlation function $R_{i,k}(\delta)$ 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. □

From the difference-balancedness of the binary constituent sequence with ideal autocorrelation property, it is clear that each sequence $h_i(x)$, $i \ne 0$ in the set $\mathcal{H}$ in Theorem 9 is balanced. It also holds for $m_i(x)$, $i \ne 0$ in Theorem 4 and $g_i(x)$, $i \ne 0$ in Theorem 7.

When we replace $f(x)$ by $\bar{f}(x)$, the 1's complement of $f(x)$ in Theorem 9, we can also obtain another LCZ sequence set $\mathcal{H}'$ in the following corollary.

*Corollary 10:* Let $n$ and $e$ be positive integers such that $e|n$. Let $\bar{f}(x)$ be the 1's complement of $f(x)$ in Theorem 9. Let $r$ be an integer such that $\gcd(r, 2^e-1) = 1$ and $1 \le r \le 2^e-2$. Let $\beta$ be a primitive element in $F_{2^e}$. Let $\mathcal{H}'$ be the family of $2^e-1$ quaternary sequences defined by the functions

$$\begin{aligned} h_0'(x) &= 2f'([\mathrm{tr}_e^n(x)]^r) \\ h_i'(x) &= f'([\mathrm{tr}_e^n(x)]^r) \boxplus 2f'([\beta^i \mathrm{tr}_e^n(x)]^r). \end{aligned}$$

Then, $\mathcal{H}'$ is a $(2^n-1, 2^e-1, (2^n-1)/(2^e-1), 1)$ LCZ sequence set. □

Note that the sequences $h_i'(x)$, $i \ne 0$ in the above corollary are not balanced.

## 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] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math*, vol. 14, pp. 614–625, 1962.

[3] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Amsterdam, The Netherlands: Elservier, 1998.

[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] 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, 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] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. 30, pp. 548–553, May 1984.

[9] 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.