New Constructions of Quaternary Low Correlation Zone Sequences

Sang-Hyo Kim, Ji-Woong Jang, Jong-Seon No, *Member, IEEE*, and Habong Chung, *Member, IEEE*

***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 Gordon–Mills–Welch (GMW) sequences are derived.**

***Index Terms*—Extended sequences, low correlation zone (LCZ) sequences, quaternary sequences, sequences.**

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 [2], multiple chip time delay among different users is allowed, which gives 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 the origin rather than to minimize the overall maximum nontrivial correlation value [8]. 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 [8]. 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 [8] proposed a binary LCZ sequence set by using Gordon–Mills–Welch (GMW) sequences [12]. For a prime p, Tang and Fan [14] proposed p-ary LCZ sequences by extending the alphabet size of each sequence in Long's work [8]. Also, they constructed p-ary LCZ sequences by using interleaved sequences [15].

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 [16]. The correlation distributions of these new quaternary LCZ sequences constructed from m-sequences and GMW sequences are derived.

Manuscript received June 3, 2004; revised December 28, 2004. This work was supported by the Korean Ministry of Information and Communications.

S.-H. Kim, J.-W. Jang, and J.-S. No are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: kimsh@ccl.snu.ac.kr; stasera@ccl.snu.ac.kr; jsno@snu.ac.kr).

H. Chung is with the School of Electronics and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@hongik.ac.kr).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2005.844068

II. Preliminaries

In this section, we introduce some definitions and notations.

Let F_{2^n} be the finite field with 2^n elements. The trace function $\mathrm{tr}_m^n(\cdot)$ from F_{2^n} to F_{2^m} is defined by

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{mi}}$$

where $x \in F_{2^n}$ and $m \mid n$. 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 $a, b \in F_{2^m}$, $x, y \in F_{2^n}$

ii) $\mathrm{tr}_m^n(x^{2^m}) = \mathrm{tr}_m^n(x)$, for all $x \in F_{2^n}$.

It is well known that $\mathrm{tr}_1^n(\alpha^t)$ is a binary m-sequence of period $2^n - 1$, where α is a primitive element in F_{2^n}.

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 α^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."

For $\delta \in F_{2^n}^*$, the cross-correlation function between two quaternary sequences $s_i(x)$ and $s_j(x)$ is defined as

$$R_{i,j}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{s_i(x\delta) - s_j(x)}$$

where w_4 is a complex fourth root of unity.

Let $f(x)$ be a mapping from F_{2^n} onto F_{2^e}, where $e \mid n$. 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 $\{f(x) \mid x \in F_{2^n}^*\}$. 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 pointed out in [5] and [9] that the binary sequence with difference-balance property has the ideal autocorrelation property necessarily and sufficiently.

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

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

Applying the 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

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

and

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

where $x \in F_{2^n}^*$. Then, the mappings ϕ and ψ 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 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

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

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

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

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

Proof: It is clear that

$$\sum_{x \in F_{2^n}} \omega_4^{s(x)} = (N_s(0) - N_s(2)) + j(N_s(1) - N_s(3))$$

and

$$N_{\psi_s}(1) = N_s(2) + N_s(3) \tag{6}$$
$$N_{\psi_s}(0) = 2^n - N_{\psi_s}(1) = N_s(0) + N_s(1) \tag{7}$$
$$N_{\mu_s}(1) = N_s(1) + N_s(2). \tag{8}$$

From (6)–(8), we have

$$\begin{aligned}N_s(0) - N_s(2) &= N_{\psi_s}(0) - N_{\mu_s}(1)\\ N_s(1) - N_s(3) &= N_{\mu_s}(1) - N_{\psi_s}(1).\end{aligned}$$

Thus, we prove the lemma. □

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.

Proof: Assume that

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

From (5), we have

$$N_{\psi_s}(0) = N_{\mu_s}(1) = N_{\psi_s}(1).$$

Thus, $N_{\psi_s}(0) = N_{\psi_s}(1) = 2^{n-1}$ and $N_{\mu_s}(1) = 2^{n-1}$. Therefore, functions $\psi_s(x)$ and $\mu_s(x)$ are balanced. The converse is manifest. □

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 $a \in F_{2^n} \backslash F_2$. Most of sequences in this paper are constructed in this manner. We can derive the cross-correlation 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 $a, b \in F_{2^n} \backslash F_2$. Then, their correlation values are given as

$$R_{a,b}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{m_a(\delta x) - m_b(x)}$$
$$= \begin{cases} 2^n - 1, & a = b \text{ and } \delta = 1\\ -1 + 2^{n-1}, & a \neq b \text{ and } \delta = \frac{b}{a} \text{ or } \frac{b+1}{a+1}\\ -1 + j2^{n-1}, & \delta = \frac{b+1}{a}\\ -1 - j2^{n-1}, & \delta = \frac{b}{a+1}\\ -1, & \text{otherwise .}\end{cases}$$

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

$$R_{a,b}(\delta) = \sum_{x \in F_{2^n}^*} w_4^{d(x)} = -1 + \sum_{x \in F_{2^n}} w_4^{d(x)}. \tag{9}$$

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

$$\begin{aligned}
S_{\psi_d}(\delta) &= \sum_{x \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((\delta a+1+b)x)} \\
&= N_{\psi_d}(0) - N_{\psi_d}(1) \qquad (10) \\
S_{\mu_d}(\delta) &= \sum_{x \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n((\delta(a+1)+b)x)} \\
&= N_{\mu_d}(0) - N_{\mu_d}(1). \qquad (11)
\end{aligned}$$

It is clear that the mapping $\psi_d(x)$ is balanced if and only if $S_{\psi_d}(\delta) = 0$.

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 $\delta \in F_{2^n} \backslash F_2$. 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 (10) and (11) are the values of trace transform 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 [4, Theorem 6.2]). Now we have to examine the bilinear form of $k(x)$ to compute the rank of the quadratic Boolean function $k(x)$ [6]. The bilinear form of $k(x)$ is given by

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

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

$$\mathrm{tr}_1^n(\delta y) = 0 \quad \text{and} \quad \mathrm{tr}_1^n(y) = 0 \tag{12}$$

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 [4, Theorem 6.2], we have

$$\begin{aligned}
K(\lambda) &= \sum_{x \in F_{2^n}} (-1)^{\mathrm{tr}_1^n(\delta x)\mathrm{tr}_1^n(x) + \mathrm{tr}_1^n(\lambda x)} \\
&= \begin{cases} 0, & 2^n - 4 \text{ times} \\ 2^{n-1}, & 3 \text{ times} \\ -2^{n-1}, & \text{once.} \end{cases} \qquad (13)
\end{aligned}$$

It is not difficult to derive the values of λ which yields 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

$$K(\lambda) = \begin{cases} 2^{n-1}, & \lambda = 0, 1, \delta \\ -2^{n-1}, & \lambda = 1 + \delta \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

Since $S_\psi(\delta)$ and $S_\mu(\delta)$ are $K(\lambda)$ evaluated at $\lambda = \delta a + 1 + b$ and $\delta(a+1) + b$, respectively, (14) can be rewritten as

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

and

$$S_{\mu_d}(\delta) = \begin{cases} 2^{n-1}, & \delta = \frac{b}{a+1}, \frac{b+1}{a+1}, \frac{b}{a} \\ -2^{n-1}, & \delta = \frac{b+1}{a} \\ 0, & \text{otherwise} \end{cases} \tag{16}$$

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

Finally, from (10), (11), (15), and (16), 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 $\delta \in F_{2^n} \backslash F_2$, we have

$$S_{\psi_d}(\delta) = \begin{cases} 2^{n-1}, & \delta = \frac{a+1}{a} \\ -2^{n-1}, & \delta = \frac{a}{a+1} \\ 0, & \text{otherwise} \end{cases} \tag{17}$$

and

$$S_{\mu_d}(\delta) = \begin{cases} 2^{n-1}, & \delta = \frac{a}{a+1} \\ -2^{n-1}, & \delta = \frac{a+1}{a} \\ 0, & \text{otherwise.} \end{cases} \tag{18}$$

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 four values of δ, the cross-correlation 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 $e\mid n$. Let β be a primitive element in F_{2^e} and $T=(2^n-1)/(2^e-1)$. Let

$$\mathcal{M}=\{m_i(x)\mid 0\le i\le 2^e-2,\ x\in F_{2^n}^*\}$$

be the set of sequences defined by the functions

$$\begin{aligned}m_0(x)&=2\mathrm{tr}_1^n(x)\\ m_i(x)&=\mathrm{tr}_1^n(x)\boxplus 2\mathrm{tr}_1^n(\beta^i x),\ \text{for } 1\le i\le 2^e-2.\end{aligned}\quad(19)$$

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

$$R_{i,k}(\delta)=\sum_{x\in F_{2^n}^*}w_4^{m_i(\delta x)-m_k(x)}$$

$$=\begin{cases}2^n-1, & 2^e-1\text{ times}\\ -1+j2^{n-1}, & (2^e-2)^2\text{ times for }\delta\notin F_{2^e}\setminus F_2\\ -1-j2^{n-1}, & (2^e-2)^2\text{ times for }\delta\notin F_{2^e}\setminus F_2\\ -1+2^{n-1}, & 2(2^e-2)(2^e-3)\text{ times for }\delta\notin F_{2^e}\setminus F_2\\ 2^{n-1}-1+j2^{n-1}, & 2(2^e-2)\text{ times for }\delta\notin F_{2^e}\setminus F_2\\ 2^{n-1}-1-j2^{n-1}, & 2(2^e-2)\text{ times for }\delta\notin F_{2^e}\setminus F_2\\ -1, & \text{otherwise}\end{cases}\quad(20)$$

as δ 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

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

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

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

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

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

Case 3) $i\ne 0$ 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

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

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

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

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

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

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

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

Let $a=\beta^i$ and $b=\beta^k$. The cross-correlation 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

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

Note that $(b+1)/a, b/a, (b+1)/(a+1)$, and $b/(a+1)$ are elements in the subfield F_{2^e}, and thus they are of the form α^{iT} for some nonzero integer i. Therefore, given any pair of sequences in the set $\mathcal{M}$, the correlation functions have the low correlation zone $(-T,T)$. We can derive (20) by combining the above five cases. □

Example 5: Let $n=4$, $e=m=2$, and $T=(2^n-1)/(2^e-1)=5$. Let α be a primitive element in F_{2^4}. Then the following set $\mathcal{M}$ is the quaternary LCZ sequences set with parameters $(15,3,5,1)$:

$$\mathcal{M}=\{m_i(x)\mid 0\le i\le 2,\ x\in F_{2^4}^*\}$$

where $m_i(x)=m_i(\alpha^t)$ is given as

$$\begin{aligned}t&=0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\\ m_0(\alpha^t)&=0,0,0,2,0,0,2,2,0,2,\ 0,\ 2,\ 2,\ 2,\ 2\\ &=2\mathrm{tr}_1^4(\alpha^t)\\ m_1(\alpha^t)&=0,2,2,1,2,0,3,3,2,3,\ 0,\ 1,\ 1,\ 3,\ 1\\ &=\mathrm{tr}_1^4(\alpha^t)\boxplus 2\mathrm{tr}_1^4(\alpha^T\alpha^t)\\ m_2(\alpha^t)&=0,2,2,3,2,0,1,1,2,1,\ 0,\ 3,\ 3,\ 1,\ 3\\ &=\mathrm{tr}_1^4(\alpha^t)\boxplus 2\mathrm{tr}_1^4(\alpha^{2T}\alpha^t)\end{aligned}$$

and $R_{i,k}(\delta)$ is given as

$$\begin{aligned}\tau&=(\ldots,-4,-3,-2,-1,\ 0,\ 1,\ 2,\ 3,\ 4,\ldots)\\ R_{0,0}(\delta)&=R_{0,0}(\alpha^\tau)\\ &=(\ldots,-1,-1,-1,-1,\ 15,-1,-1,-1,-1,\ldots)\end{aligned}$$

$$
\begin{aligned}
R_{1,1}(\delta) &= R_{1,1}(\alpha^\tau) \\
&= (\ldots, -1, -1, -1, -1,\ 15, -1, -1, -1, -1, \ldots) \\
R_{2,2}(\delta) &= R_{2,2}(\alpha^\tau) \\
&= (\ldots, -1, -1, -1, -1,\ 15, -1, -1, -1, -1, \ldots) \\
R_{0,1}(\delta) &= R_{0,1}(\alpha^\tau) \\
&= (\ldots, -1, -1, -1, -1, -1, -1, -1, -1, -1, \ldots) \\
R_{0,2}(\delta) &= R_{0,2}(\alpha^\tau) \\
&= (\ldots, -1, -1, -1, -1, -1, -1, -1, -1, -1, \ldots) \\
R_{1,2}(\delta) &= R_{1,2}(\alpha^\tau) \\
&= (\ldots, -1, -1, -1, -1, -1, -1, -1, -1, -1, \ldots).
\end{aligned}
$$

□

Tang, Fan, and Matsufuji [16] derived the lower bound on the correlation of LCZ sequences using the Welch bound [17].

Theorem 6 (Tang, Fan, and Matsufuji [16]): Let $\mathcal{S}$ be an LCZ sequence set with parameters (N, M, L, ϵ). Then

$$ML - 1 \le \frac{N-1}{1-\epsilon^2/N}. \tag{21}$$

□

Now we can check the optimality of our quaternary LCZ sequence set $\mathcal{M}$.

Corollary 7: The set $\mathcal{M}$ is optimal with respect to the Tang–Fan–Matsufuji bound given in Theorem 6.

Proof: The proof is straightforward. By substituting $N = 2^n - 1$, $M = 2^e - 1$, and $\epsilon = 1$ in (21), we have

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

and thus,

$$L \le \frac{2^n}{2^e - 1}.$$

Since L is an integer, we have

$$L \le \left\lfloor \frac{2^n}{2^e - 1} \right\rfloor = \frac{2^n - 1}{2^e - 1} = T.$$

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

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 [7] 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

$$H(yx) = y^d H(x) \tag{22}$$

for any $y \in F_{p^e}$ and $x \in F_{p^n}$.

Lemma 8: Let m, e, and n be positive integers such that $n = em$. Let $q = 2^e$ and $A = \{1, \alpha, \ldots, \alpha^{T-1}\}$, where α 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 $\delta \in F_{q^m} \backslash F_q$, let $M_\delta(a, b)$ be the number of $x_2 \in A$ satisfying

$$v(\delta x_2) = a \quad \text{and} \quad v(x_2) = b, \ \ a, b \in F_q. \tag{23}$$

Then, we have

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

Proof: Let $N_\delta(a, b)$ be the number of $x \in F_{q^m}^*$ satisfying $v(\delta x) = a$ and $v(x) = b$. Let $x = x_1 x_2$, where $x_1 \in F_q$ and $x_2 \in A$. Because $v(x)$ is difference-balanced, $v(\delta x) - v(cx) = v(\delta x) - cv(x)$ is balanced for any $c \in F_q^*$ and 0 occurs $q^{m-1} - 1$ times as x varies over $F_{q^m}^*$. Thus, we have

$$\sum_{a \in F_q} N_\delta(ca, a) = q^{m-1} - 1. \tag{24}$$

Since $v(x)$ is balanced, we have

$$\sum_{a \in F_q} N_\delta(a, 0) = \sum_{b \in F_q} N_\delta(0, b) = q^{m-1} - 1. \tag{25}$$

Also, note that

$$\sum_{a \in F_q} \sum_{b \in F_q} N_\delta(a, b) = q^m - 1. \tag{26}$$

Now, we have

$$
\begin{aligned}
\sum_{a \in F_q} \sum_{b \in F_q} N_\delta(a, b) &= \sum_{a \in F_q} N_\delta(a, 0) + \sum_{b \in F_q} N_\delta(0, b) \\
&\quad - N_\delta(0, 0) + \sum_{c \in F_q^*} \sum_{a \in F_q^*} N_\delta(a, ca) \\
&= \sum_{a \in F_q} N_\delta(a, 0) + \sum_{b \in F_q} N_\delta(0, b) - N_\delta(0, 0) \\
&\quad + \sum_{c \in F_q^*} \left\{ \sum_{a \in F_q} N_\delta(a, ca) - N_\delta(0, 0) \right\}.
\end{aligned} \tag{27}
$$

Plugging (24)–(26) into (27), we have

$$N_\delta(0, 0) = q^{m-2} - 1. \tag{28}$$

From (24) and (28), we also have

$$\sum_{a \in F_q^*} N_\delta(ca, a) = \sum_{a \in F_q} N_\delta(ca, a) - N_\delta(0, 0) = q^{m-2}(q - 1). \tag{29}$$

Let $\beta = \alpha^T$. For a given x_2 such that $v(\delta x_2) = cv(x_2)$, the ordered pair $(v(\delta x), v(x)) = (x_1 v(\delta x_2), x_1 v(x_2))$ takes each value in the list

$$(c, 1), (c\beta, \beta), \ldots, (c\beta^{q-2}, \beta^{q-2})$$

exactly once as x_1 varies over F_q^*. Therefore, we have

$$\sum_{a \in F_q^*} N_\delta(ca, a) = (q - 1) \sum_{a \in F_q^*} M_\delta(ca, a)$$

which, in turn, tells us that

$$\sum_{a\in F_q^*} M_\delta(ca,a) = q^{m-2}.$$

Similarly, we have

$$M_\delta(0,0) = \frac{N_\delta(0,0)}{q-1} = \frac{q^{m-2}-1}{q-1}$$
$$\sum_{c\in F_q^*} M_\delta(c,0) = \frac{\sum_{c\in F_q^*} N_\delta(c,0)}{q-1} = q^{m-2}$$
$$\sum_{c\in F_q^*} M_\delta(0,c) = \frac{\sum_{c\in F_q^*} N_\delta(0,c)}{q-1} = q^{m-2}. \qquad \square$$

Theorem 9: Let n and e be positive integers such that $e \mid n$ 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

$$\mathcal{G} = \{g_i(x) \mid 0 \le i \le 2^e-2,\ x \in F_{2^n}^*\}$$

of quaternary sequences defined by

$$g_0(x) = 2\mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^r)$$
$$g_i(x) = \mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^r) \boxplus 2\mathrm{tr}_1^e([\beta^i \mathrm{tr}_e^n(x)]^r), \quad 1 \le i \le 2^e-2 \tag{30}$$

where β 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: What we are going to show is that there is a 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 $\mathcal{M}$. Also, we will show that the sequence $m_{ri}(x)$ of $\mathcal{M}$ given in (19) is the one that corresponds to the sequence $g_i(x)$ of $\mathcal{G}$ given in (30). Let $a = \beta^i$ and $b = \beta^k$. For nonzero i and k, we have

$$m_{ri}(x) = \mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(a^r x)$$
$$m_{rk}(x) = \mathrm{tr}_1^n(x) \boxplus 2\mathrm{tr}_1^n(b^r x)$$

and

$$g_i(x) = \mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^r) \boxplus 2\mathrm{tr}_1^e([a\mathrm{tr}_e^n(x)]^r)$$
$$g_k(x) = \mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^r) \boxplus 2\mathrm{tr}_1^e([b\mathrm{tr}_e^n(x)]^r)$$

and $m_0(x)$ corresponds to $g_0(x)$. Let

$$A = \{\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{T-1}\}.$$

For $\delta = (\delta_1\delta_2)$ and $\delta' = (\delta_1^r\delta_2)$ in $F_{2^n}^*$ such that $\delta_1 \in F_{2^e}^*$ and $\delta_2 \in A$, define

$$R_m(\delta') = \sum_{x\in F_{2^n}^*} \omega_4^{m_{ri}(\delta' x) - m_{rk}(x)}$$

$$R_g(\delta) = \sum_{x\in F_{2^n}^*} \omega_4^{g_i(\delta x) - g_k(x)}.$$

Now we are going to investigate the values of $R_g(\delta)$ from those of $R_m(\delta')$ given in Theorem 4. We have to consider the following cases.

Case 1) $i \ne k$, $i \ne 0$, and $k \ne 0$:

By substituting $x = x_1x_2$, $\delta = \delta_1\delta_2$, such that $x_1, \delta_1 \in F_{2^e}^*$ and $x_2, \delta_2 \in A$, we can rewrite $R_m(\delta')$ and $R_g(\delta)$ as

$$R_m(\delta') = \sum_{x_2\in A}\sum_{x_1\in F_{2^e}^*} w_4^{\{\mathrm{tr}_1^e(x_1\delta_1^r[\mathrm{tr}_e^n(\delta_2x_2)]) \boxplus 2\mathrm{tr}_1^e(x_1\delta_1^r a^r[\mathrm{tr}_e^n(\delta_2x_2)])\}} \times w_4^{-\{\mathrm{tr}_1^e(x_1[\mathrm{tr}_e^n(x_2)]) \boxplus 2\mathrm{tr}_1^e(x_1 b^r[\mathrm{tr}_e^n(x_2)])\}} \tag{31}$$

and

$$R_g(\delta) = \sum_{x_2\in A}\sum_{x_1\in F_{2^e}^*} w_4^{\{\mathrm{tr}_1^e(x_1\delta_1^r[\mathrm{tr}_e^n(\delta_2x_2)]^r) \boxplus 2\mathrm{tr}_1^e(x_1\delta_1^r a^r[\mathrm{tr}_e^n(\delta_2x_2)]^r)\}} \times w_4^{-\{\mathrm{tr}_1^e(x_1[\mathrm{tr}_e^n(x_2)]^r) \boxplus 2\mathrm{tr}_1^e(x_1 b^r[\mathrm{tr}_e^n(x_2)]^r)\}}. \tag{32}$$

Let us separate the outer summation $\sum_{x_2\in A}$ in (31) and (32) into the sum of two partial summations as

$$\sum_{x_2\in A} = \sum_{\substack{x_2\in A \\ \mathrm{tr}_e^n(\delta x_2)\ne 0 \\ \mathrm{tr}_e^n(x_2)\ne 0}} + \sum_{\substack{x_2\in A \\ \mathrm{tr}_e^n(\delta x_2)= 0 \\ \text{or } \mathrm{tr}_e^n(x_2)= 0}}.$$

i) For the summation over $x_2 \in A$ such that $\mathrm{tr}_e^n(\delta x_2) \ne 0$ and $\mathrm{tr}_e^n(x_2) \ne 0$:

For a given x_2, let $\xi_{x_2} = \mathrm{tr}_e^n(\delta_2x_2)$ and $\zeta_{x_2} = \mathrm{tr}_e^n(x_2)$. Then the inner summation of (31) is rewritten as

$$\sum_{x_1\in F_{2^e}^*} w_4^{\{\mathrm{tr}_1^e(x_1\delta_1^r\xi_{x_2}) \boxplus 2\mathrm{tr}_1^e(x_1\delta_1^r\xi_{x_2}a^r)\} - \{\mathrm{tr}_1^e(x_1\zeta_{x_2}) \boxplus 2\mathrm{tr}_1^e(x_1\zeta_{x_2}b^r)\}}$$

which is the cross correlation $R_{a^r,b^r}(\delta_1^r\xi_{x_2}/\zeta_{x_2})$ of two quaternary sequences of period 2^e-1, namely,

$$\mathrm{tr}_1^e(x_1) \boxplus 2\mathrm{tr}_1^e(a^r x_1) \quad \text{and} \quad \mathrm{tr}_1^e(x_1) \boxplus 2\mathrm{tr}_1^e(b^r x_1).$$

Similarly, we can see the inner summation of (32) is nothing but $R_{a^r,b^r}([\delta_1\xi_{x_2}/\zeta_{x_2}]^r)$. From Theorem 3, $R_{a^r,b^r}(\delta_1^r\xi_{x_2}/\zeta_{x_2})$ takes value -1 except for the cases of

$$\frac{\delta_1^r\xi_{x_2}}{\zeta_{x_2}} = \delta_1^r\frac{\mathrm{tr}_e^n(\delta_2x_2)}{\mathrm{tr}_e^n(x_2)} = \frac{b^r}{a^r},\ \frac{b^r+1}{a^r+1},\ \frac{b^r}{a^r+1},\ \text{or}\ \frac{b^r+1}{a^r}$$

as x_2 varies over A. Similarly, $R_{a^r,b^r}\left(\delta_1^r\xi_{x_2}^r/\zeta_{x_2}^r\right)$ also takes value -1 except for the cases of

$$\frac{\delta_1^r\xi_{x_2}^r}{\zeta_{x_2}^r} = \delta_1^r\left(\frac{\mathrm{tr}_e^n(\delta_2x_2)}{\mathrm{tr}_e^n(x_2)}\right)^r = \frac{b^r}{a^r},\ \frac{b^r+1}{a^r+1},\ \frac{b^r}{a^r+1},\ \text{or}\ \frac{b^r+1}{a^r}$$

as x_2 varies over A.

But due to Lemma 8, we know that the number of $x_2 \in A$ satisfying

$$\frac{\mathrm{tr}_e^n(\delta_2x_2)}{\mathrm{tr}_e^n(x_2)} = g$$

is exactly 2^{n-2e} for any $g \in F_{2^e}^*$. Thus, we have

$$\sum_{\substack{x_2 \in A \\ \mathrm{tr}_e^n(\delta x_2)\neq 0 \\ \mathrm{tr}_e^n(x_2)\neq 0}} \sum_{x_1 \in F_{2^e}^*} \omega_4^{m_{ri}(\delta' x)-m_{rk}(x)} = \sum_{\substack{x_2 \in A \\ \mathrm{tr}_e^n(\delta x_2)\neq 0 \\ \mathrm{tr}_e^n(x_2)\neq 0}} \sum_{x_1 \in F_{2^e}^*} \omega_4^{g_i(\delta x)-g_k(x)}.$$

ii) For the summation over $x_2 \in A$ such that $\mathrm{tr}_e^n(\delta x_2) = 0$ or $\mathrm{tr}_e^n(x_2) = 0$:

In this case, it is easy to see that both of the inner summations in (31) and (32) are the same as

$$\sum_{x_1 \in F_{2^e}^*} \omega_4^{\mathrm{tr}_1^e(x_1) \boxplus 2\mathrm{tr}_1^e(a^r x_1)}, \text{ if } \mathrm{tr}_e^n(\delta x_2) \neq 0, \ \mathrm{tr}_e^n(x_2) = 0$$

or

$$\sum_{x_1 \in F_{2^e}^*} \omega_4^{\mathrm{tr}_1^e(x_1) \boxplus 2\mathrm{tr}_1^e(b^r x_1)}, \text{ if } \mathrm{tr}_e^n(\delta x_2) = 0, \ \mathrm{tr}_e^n(x_2) \neq 0$$

or

$$2^e - 1, \text{ if } \mathrm{tr}_e^n(\delta x_2) = 0, \ \mathrm{tr}_e^n(x_2) = 0.$$

Therefore, we have $R_m(\delta') = R_g(\delta)$.

Case 2) $i = 0, k = 0$:

This is the case of the autocorrelation of binary m-sequences for $R_m(\delta')$ and GMW sequences for $R_g(\delta)$.

Case 3) $i = k \neq 0$:

This is the case of autocorrelation. From Theorem 3, we have $R_m(\delta') = R_g(\delta)$.

Case 4) $i \neq 0$ and $k = 0$ (or $i = 0$ and $k \neq 0$):

In this case, only one quaternary sequence remains in the exponent of ω_4. It is easily checked that $R_m(\delta) = R_g(\delta')$.

Consequently, we have $R_m(\delta') = R_g(\delta)$. Therefore, $\mathcal{G}$ is a $(2^n - 1, 2^e - 1, T, 1)$ LCZ sequence set. □

Example 10: Let $n = 6$, $e = 3$, $m = 2$, $r = 3$, and $T = (2^n - 1)/(2^e - 1) = 9$. Let α be a primitive element in F_{2^6}. Then the following sequence set $\mathcal{G}$ is the quaternary LCZ sequence set with parameters $(63, 7, 9, 1)$:

$$\mathcal{G} = \{g_i(x) \mid 0 \le i \le 2^3 - 2, \ x \in F_{2^6}^*\}$$

where $g_i(x)$ is given as

$$\begin{aligned}
g_0(x) &= 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(x)]^3) \\
&= 000002020020022202022020020222 \\
&\quad 000220022222200200202220022202 00 \\
g_1(x) &= \mathrm{tr}_1^3([\mathrm{tr}_3^6(x)]^3) \boxplus 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^T x)]^3) \\
&= 020023212032213103033301023013 3 \\
&\quad 222310211313320122303110011121 20 \\
g_2(x) &= \mathrm{tr}_1^3([\mathrm{tr}_3^6(x)]^3) \boxplus 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{2T} x)]^3) \\
&= 022203012032211123013323221031 1 \\
&\quad 202330033313100100121310211323 02
\end{aligned}$$

$$\begin{aligned}
g_3(x) &= \mathrm{tr}_1^3([\mathrm{tr}_3^6(x)]^3) \boxplus 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{3T} x)]^3) \\
&= 022201032012233321031121223013 3 \\
&\quad 202110011131300300323130231231 02 \\
g_4(x) &= \mathrm{tr}_1^3([\mathrm{tr}_3^6(x)]^3) \boxplus 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{4T} x)]^3) \\
&= 002223230030031323013321201011 1 \\
&\quad 020310211333120322121130233101 22 \\
g_5(x) &= \mathrm{tr}_1^3([\mathrm{tr}_3^6(x)]^3) \boxplus 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{5T} x)]^3) \\
&= 020021232012231301011103021031 1 \\
&\quad 222130233131120322101330033323 20 \\
g_6(x) &= \mathrm{tr}_1^3([\mathrm{tr}_3^6(x)]^3) \boxplus 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{6T} x)]^3) \\
&= 002221210010013121031123203033 3 \\
&\quad 020130233111320122323310211303 22.
\end{aligned}$$

□

No, Yang, Chung, and Song constructed *extended sequences* with ideal autocorrelation property from sequences of short period with ideal autocorrelation property [11]. We use the *extended sequences* to construct LCZ sequence sets.

Lemma 11: Let $f(x)$ be a function from F_{2^e} to F_2 with balance and difference-balance property and $f(0) = 0$. For $a, b \in F_{2^e} \backslash F_2$, 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

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

Proof: From (3) and (4), S_{ψ_d} can be rewritten as

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

Now, let $I_1(x)$ and $I_2(x)$ be the inner summation

$$\sum_{\delta \in F_{2^e}^*} (-1)^{f(\delta x)f(x)+f(x)+f(bx)+f(a\delta x)}$$

for the cases when $f(x) = 0$ and $f(x) = 1$, respectively, i.e.,

$$I_1(x) = \sum_{\delta \in F_{2^e}^*} (-1)^{f(bx)+f(a\delta x)}$$

and

$$I_2(x) = \sum_{\delta \in F_{2^e}^*} (-1)^{f(\delta x)+1+f(bx)+f(a\delta x)}.$$

Then S_{ψ_d} can be expressed as

$$S_{\psi_d} = \sum_{x \in \{x \mid f(x)=0, x \in F_{2^e}^*\}} I_1(x) + \sum_{x \in \{x \mid f(x)=1, x \in F_{2^e}^*\}} I_2(x). \quad (33)$$

The first term in (33) is computed as

$$\sum_{x\in\{x|f(x)=0,x\in F_{2^e}^*\}} I_1(x) = \sum_{x\in\{x|f(x)=0,x\in F_{2^e}^*\}} (-1)^{f(bx)} \sum_{\delta\in F_{2^e}^*} (-1)^{f(a\delta x)} = \sum_{x\in\{x|f(x)=0,x\in F_{2^e}^*\}} (-1)^{f(bx)+1}$$

since $f(x)$ is balanced.

The second term in (33) is computed as

$$\sum_{x\in\{x|f(x)=1,x\in F_{2^e}^*\}} I_2(x) = \sum_{x\in\{x|f(x)=1,x\in F_{2^e}^*\}} (-1)^{f(bx)+1} \times \sum_{\delta\in F_{2^e}^*} (-1)^{f(\delta x)+f(a\delta x)} = \sum_{x\in\{x|f(x)=1,x\in F_{2^e}^*\}} (-1)^{f(bx)}$$

since $f(x)$ is difference-balanced.

Thus, we have

$$S_{\psi_d} = \sum_{x\in\{x|f(x)=1,x\in F_{2^e}^*\}} (-1)^{f(bx)} - \sum_{x\in\{x|f(x)=0,x\in F_{2^e}^*\}} (-1)^{f(bx)}.$$

Finally, from the difference balance property, we have

$$(f(x), f(bx)) = \begin{cases} (0,0), & 2^{e-2}-1 \text{ times} \\ (1,0), & 2^{e-2} \text{ times} \\ (0,1), & 2^{e-2} \text{ times} \\ (1,1), & 2^{e-2} \text{ times} \end{cases}$$

as x varies over $F_{2^e}^*$. Therefore, we have

$$S_{\psi_d} = 1.$$

The proof for $S_{\mu_d} = 1$ goes the same way and we omit the detailed proof. □

Theorem 12 (No, Yang, Chung, and Song [11]): Let n and e be positive integers such that $e \mid n$. 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 $1 \le r \le 2^e-2$. Then the sequence of period 2^n-1 defined by

$$f([\mathrm{tr}_e^n(x)]^r)$$

has the ideal autocorrelation property. □

Using the extended sequences in the above theorem, we can construct LCZ sequences as in the following theorem.

Theorem 13: Let n and e be positive integers such that $e \mid n$. 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 β be a primitive element in F_{2^e}. Let $\mathcal{H}$ be the set of 2^e-1 quaternary sequences defined by the functions

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

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

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

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

$$R_{i,k}(\delta) = \sum_{x\in F_{2^n}^*} \omega_4^{h_i(\delta x)-h_k(x)} = \sum_{x_2\in A} \sum_{x_1\in F_{2^e}^*} \omega_4^{\{f(x_1^r[\mathrm{tr}_e^n(\delta x_2)]^r)\boxplus 2f(x_1^r a^r[\mathrm{tr}_e^n(\delta x_2)]^r)\}} \times \omega_4^{-\{f(x_1^r[\mathrm{tr}_e^n(x_2)]^r)\boxplus 2f(x_1^r b^r[\mathrm{tr}_e^n(x_2)]^r)\}}.$$

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 8, $R_{i,k}(\delta)$ is rewritten as

$$\begin{aligned} R_{i,k}(\delta) &= \sum_{d\in F_{2^e}^*} M_\delta(cd,d) \sum_{c\in F_{2^e}^*} \sum_{x_1\in F_{2^e}^*} \omega_4^{\{f([x_1cd]^r)\boxplus 2f([x_1acd]^r)\}} \times \omega_4^{-\{f([x_1d]^r)\boxplus 2f([x_1bd]^r)\}} \\ &\quad + M_\delta(0,0) \sum_{x_1\in F_{2^e}^*} \omega_4^0 \\ &\quad + \sum_{c\in F_{2^e}^*} M_\delta(c,0) \sum_{x_1\in F_{2^e}^*} \omega_4^{\{f([x_1c]^r)\boxplus 2f([x_1ac]^r)\}} \\ &\quad + \sum_{c\in F_{2^e}^*} M_\delta(0,c) \sum_{x_1\in F_{2^e}^*} \omega_4^{-\{f([x_1c]^r)\boxplus 2f([x_1bc]^r)\}} \\ &= 2^{n-2e} \sum_{c\in F_{2^e}^*} \sum_{x_1\in F_{2^e}^*} \omega_4^{\{f([x_1c]^r)\boxplus 2f([x_1ac]^r)\}} \times \omega_4^{-\{f(x_1^r)\boxplus 2f([x_1b]^r)\}} \\ &\quad + \frac{2^{n-2e}-1}{2^e-1} \sum_{x_1\in F_{2^e}^*} \omega_4^0 \\ &\quad + 2^{n-2e} \sum_{x_1\in F_{2^e}^*} \omega_4^{\{f([x_1c]^r)\boxplus 2f([x_1ac]^r)\}} \\ &\quad + 2^{n-2e} \sum_{x_1\in F_{2^e}^*} \omega_4^{-\{f([x_1c]^r)\boxplus 2f([x_1bc]^r)\}}. \end{aligned}$$

From Lemmas 1 and 11, $R_{i,k}(\delta)$ 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

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

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

Case 2) $i = k$:

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

$$\begin{aligned} R_{i,i}(\delta) &= 2^{n-2e} \sum_{c \in F_{2^e}^*} \sum_{x_1 \in F_{2^e}^*} \omega_4^{\{f([x_1 c]^r) \boxplus 2f([x_1 ac]^r)\}} \\ &\quad \times \omega_4^{-\{f(x_1^r) \boxplus 2f([x_1 b]^r)\}} \\ &\quad + \frac{2^{n-2e}-1}{2^e-1} \sum_{x_1 \in F_{2^e}^*} \omega_4^0 \\ &\quad + 2^{n-2e} \sum_{x_1 \in F_{2^e}^*} \omega_4^{\{f([x_1 c]^r) \boxplus 2f([x_1 ac]^r)\}} \\ &\quad + 2^{n-2e} \sum_{x_1 \in F_{2^e}^*} \omega_4^{\{f(x_1^r c^r) \boxplus 2f([x_1 bc]^r)\}} \\ &= 2^{n-2e} + 2^{n-2e} - 1 + 2 \cdot 2^{n-2e}(-1) = -1. \end{aligned}$$

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 $\delta \in F_{2^e} \backslash F_2$ and $R_{0,0}(\delta) = -1$ for $\delta \neq 1$.

Thus, the correlation function $R_{i,k}(\delta)$ takes the value -1 in the low correlation zone $\{\alpha^{-T+1}, \ldots, 1, \ldots, \alpha^{T-1}\}$ 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 $h_i(x)$, $i \neq 0$ in the set $\mathcal{H}$ in Theorem 13 is balanced. It also holds for $m_i(x)$, $i \neq 0$ in Theorem 4 and $g_i(x)$, $i \neq 0$ in Theorem 9.

When we replace $f(x)$ by $\bar{f}(x)$, the 1's complement of $f(x)$ in Theorem 13, we can also obtain another LCZ sequence set $\mathcal{H}'$ in the following corollary.

Corollary 14: Let n and e be positive integers such that $e \mid n$. Let $\bar{f}(x)$ be the 1's complement of $f(x)$ in Theorem 13. Let r be an integer such that $\gcd(r, 2^e - 1) = 1$ and $1 \leq r \leq 2^e - 2$. Let β 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 $h'_i(x)$, $i \neq 0$ in the above corollary are not balanced.

REFERENCES

[1] S. Boztas and P. V. Kumar, "Binary sequences with Gold-like correlation but larger linear span," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 532–537, Mar. 1994.

[2] R. De Gaudenzi, C. Elia, and R. Viola, "Bandlimited quasi-synchronous 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.

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

[4] 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.

[5] S.-H. Kim, H. Chung, and J.-S. No, "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, Mar. 2005.

[6] 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.

[7] 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, Mar. 1995.

[8] 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. 6, pp. 1268–1275, Nov. 1998.

[9] J.-S. No, "New cyclic difference sets with Singer parameters constructed from d-homogeneous functions," *Des., Codes Cryptogr.*, vol. 33, no. 1, pp. 23–37, 2004.

[10] 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, Sep. 2002.

[11] 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. Information Theory and its Applications (ISITA'96)*, Victoria, BC, Canada, Sep. 1996, pp. 837–840.

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

[13] N. Suehiro, "Approximately synchoronized CDMA system without cochannel using pseudo-periodic sequences," in *Proc. Int. Symp. Personal Communication '93*, Nanjing, China, Jul. 1994, pp. 179–184.

[14] 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.

[15] ——, "Large families of generalized d–form sequences with low correlations and large linear span based on the interleaved technique," preprint, 2004.

[16] 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, Mar. 2000.

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