New Constructions of Quaternary Low Correlation Zone Sequences from Binary Extended Sequence [1]

Sang-Hyo Kim, 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

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 extended sequences of the same length with ideal autocorrelation. These new sequence sets are optimal with respect to the bound by Tang, Fan, and Matsufuji.

1. 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 are 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 orgin rather than to minimize the overall maximum nontrivial correlation value[5]. 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[5]. 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[5] proposed a binary LCZ sequence set by using GMW sequences[8]. For a prime p, Tang and Fan[10] proposed p-ary LCZ sequences by extending the alphabet size of each sequence in Long's work[5].

In this paper, given a composite integer n, we propose a method of constructing quaternary LCZ sequences of period $2^n - 1$ from binary extended sequences of the same length with ideal autocorrelation by No, Chung, Yang, and Song[7]. These new sequences are optimal with respect to the bound by Tang, Fan, and Matsufuji[11].

[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 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 $m|n$. 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 crosscorrelation 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 $e|n$. 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 $\delta \in F_{2^n} \backslash \{0,1\}$. It is pointed out in [3] and [6] 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

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

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 ϕ and ψ of the quaternary sequence $d(x)$ are given by

$$\phi(d(x)) = v_1(x) + w_1(x) \tag{2}$$
$$\psi(d(x)) = v_1(x)w_1(x) + w_1(x) + w_2(x) + v_2(x). \tag{3}$$

3. Quaternary LCZ sequences constructed from binary extended sequences

In this section, we propose the method to construct the set $\mathcal{H}$ of quaternary LCZ sequences from binary extended sequences. New sequence set is optimal with the prospect to the bound by Tang, Fan, and Matsufuji[11].

The following lemmas are useful in the computation of correlation of these quaternary LCZ sequences.

Lemma 1 (Kim, Jang, No, and Chung[4]) 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

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

□

Lemma 2 (Kim, Jang, No, and Chung[4]) 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

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

□

Lemma 3 (Kim, Jang, No, and Chung[4]) 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

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

Then, we have

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

□

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.

Theorem 1 (No, Yang, Chung, and Song[7]) 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 $1 \le r \le 2^e - 2$, 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 above theorem, we can construct LCZ sequences as in the following theorem.

Theorem 2 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 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

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

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

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

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

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

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

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

From Lemma 1 and Lemma 2, $R_{i,k}(\delta)$ 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 $\delta \notin F_{2^e}$, the correlation function is given as

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

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 $\delta \in F_{2^e} \setminus F_2$ 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 $h_i(x)$, $i \neq 0$ in the set $\mathcal{H}$ in Theorem 2 is balanced.

When we replace $f(x)$ by $\bar{f}(x)$, the 1's complement of $f(x)$ in Theorem 2, we can also obtain another LCZ sequence set $\mathcal{H}'$ in the following corollary.

Corollary 1 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 2. 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.

Tang, Fan, and Matsufuji[11] derived the lower bound on the correlation of LCZ sequences using the Welch bound[12].

Theorem 3 (Tang, Fan, and Matsufuji[11]) Let $\mathcal{S}$ be a LCZ sequence set with parameter (N, M, L, ϵ). Then,

$$ML - 1 \leq \frac{N-1}{1 - \epsilon^2/N}. \tag{7}$$

□

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

Corollary 2 The set $\mathcal{H}$ is optimal with respect to the Tang-Fan-Matsufuji bound given in Theorem 3.

Proof : The proof is straightforward. By substituting $N = 2^n - 1$, $M = 2^e - 1$, and $\epsilon = 1$ in (7), we have

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

and thus

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

Since L is an integer, we have

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

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

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] 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.

[3] S.-H. Kim, J.-S. No, H. Chung, and T. Helleseth, "New cyclic relative difference sets constructed from d-homogeneous functions with difference-balance property," submitted to *IEEE Trans. Inform. Theory*, vol. 51, no 3, pp. 1155-1163 Mar. 2003.

[4] S.-H. Kim, J.-W. Jang, J.-S. No, and Habong Chung, "New construction methods of quaternary low correlation zone sequence," *preprint*, 2005.

[5] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Technol.*, vol. 47, pp. 1268–1275, Nov. 1998.

[6] J.-S. No, "New cyclic difference sets with Singer parameters constructed from d-homogeneous functions," accepted for publication in *Designs, Codes and Cryptography*, vol. 33, issue 3, pp. 199-213, November 2004.

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

[10] 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.

[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.