Binary Sequence Sets with Low Correlation Zone

Ji-Woong Jang, Jong-Seon No
School of EE and CS
Seoul National University
Seoul, Korea
Email: stasera@ccl.snu.ac.kr, jsno@snu.ac.kr

Habong Chung
School of EEE
Hongik University
Seoul, Korea
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 e and n 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.**

I. 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 [4], 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 [4].

In this paper, for integers e and n 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[6]. These new LCZ sequences use Legendre sequences as their column sequences.

II. 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 $s_i(x)$ and $s_j(x)$ be two binary sequences of period 2^n-1, defined in F_{2^n}, the finite field with 2^n elements. Then for $\delta \in F_{2^n}^*$, the correlation function between two binary sequences $s_i(x)$ and $s_j(x)$ is defined as

$$R_{i,j}(\delta)=\sum_{x\in F_{2^n}^*}(-1)^{s_i(x\delta)+s_j(x)}.$$

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 of F_{2^n}.

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

$$\begin{aligned}S(\lambda) &= \sum_{t=0}^{N-1}s(t)\alpha^{-\lambda t}\\ s(t) &= \sum_{\lambda=0}^{N-1}S(\lambda)\alpha^{\lambda t}.\end{aligned}$$

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

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

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

Klapper[3] 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 $x\in F_{p^n}$

$$H(yx)=y^dH(x). \quad (2)$$

No, Yang, Chung, and Song constructed the *extended sequences* with ideal autocorrelation property from the sequences of shorter period with ideal autocorrelation property [6].

Theorem 1 ([6]): Let e and n be positive integers such that $e|n$. Let $f(x)$ be a 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. □

Let $n = em$ and d be an integer such that $gcd(d, 2^e-1) = 1$. Let $f(x)$ be a function from F_{2^e} to F_2 with ideal autocorrelation property and the function $h(x)$ from F_{2^n} to F_{2^e} be a 1-form function over F_{2^e} with balance and difference-balance property. Then we call the function $f([h(x)]^d)$ "*extended form sequence*", where the sequence $f(x)$ is called column sequence and $h(x)$ is called phase sequence.

Lemma 2 ([2]): 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 α is a primitive element of F_{2^n} and $T = (q^m-1)/(q-1)$. Let $h(x)$ 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

$$h(\delta x_2) = a \quad \text{and} \quad h(x_2) = b, \quad a, b \in F_q. \tag{3}$$

Then, we have

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

□

Tang and Fan proposed the following theorem.

Theorem 3 ([7]): Let e and n be integers such that $e|n$. Let $f(y)$ and $g(y)$ be cyclically distinct binary sequences of period 2^e-1 from F_{2^e} to F_2 and the function $h(x)$ from F_{2^n} to F_{2^e} be a 1-form function over F_{2^e} 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

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

where $I(f) = \sum_{y \in F_{2^e}^*} (-1)^{f(y)}$ and $C_{f,g}(\delta) = \sum_{y \in F_{2^e}} (-1)^{f(\delta y)+g(y)}$.

Proof: Theorem 3 can be proven as in the following way.

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

Since $h(x)$ is a 1-form function, $h(\delta x) = \delta h(x)$. Let $N_h(a)$ be the number of $x \in F_{2^n}^*$ such that $h(x) = a$. Then we can rewrite $R_{f,g}(\delta)$ as follows

$$\begin{aligned} R_{f,g}(\delta) &= \sum_{x \in F_{2^n}^*} (-1)^{f(h(\delta x))+g(h(x))} \\ &= \sum_{x \in F_{2^n}^*} (-1)^{f(\delta h(x))+g(h(x))} \\ &= \sum_{y \in F_{2^e}} N_h(y)(-1)^{f(\delta y)+g(y)}. \end{aligned}$$

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

$$N_h(y) = \begin{cases} 2^{n-e}-1, & \text{if } y = 0 \\ 2^{n-e}, & \text{otherwise.} \end{cases}$$

Therefore, when $\delta \in F_{2^e}$, $R_{f,g}(\delta)$ is

$$R_{f,g}(\delta) = 2^{n-e}C_{f,g}(\delta) + 2^{n-e} - 1.$$

Case 2) $\delta \notin F_{2^e}$

Let $T = (2^n-1)/(2^e-1)$. Let $x = x_1x_2$, where $x_1 \in F_{2^e}$ and $x_2 \in A = \{1, \alpha, \alpha^2, \cdots, \alpha^{T-1}\}$. For $\delta \notin F_{2^e}$, with the replacement of $h(\delta x_2)$ by cd and $h(x_2)$ by d for nonzero $h(\cdot)$ and also from Lemma 2, $R_{f,g}(\delta)$ is rewritten as

$$\begin{aligned} R_{f,g}(\delta) &= \sum_{x \in F_{2n}} (-1)^{f(h(\delta x))+g(h(x))} \\ &= \sum_{c \in F_{2^e}^*} \sum_{d \in F_{2^e}^*} M_\delta(cd,d) \sum_{x_1 \in F_{2^e}^*} (-1)^{f(x_1cd)+g(x_1d)} \\ &\quad + M_\delta(0,0) \sum_{x_1 \in F_{2^e}^*} (-1)^0 \\ &\quad + \sum_{c \in F_{2^e}^*} M_\delta(c,0) \sum_{x_1 \in F_{2^e}^*} (-1)^{f(x_1c)} \\ &\quad + \sum_{c \in F_{2^e}^*} M_\delta(0,c) \sum_{x_1 \in F_{2^e}^*} (-1)^{g(x_1c)\}} \\ &= \sum_{c \in F_{2^e}^*} \sum_{d \in F_{2^e}^*} M_\delta(cd,d) \sum_{x_1 \in F_{2^e}^*} (-1)^{f(x_1cd)+g(x_1d)} \\ &\quad + 2^{n-2e} - 1 + 2^{n-2e}I(f) + 2^{n-2e}I(g). \end{aligned} \tag{4}$$

The first term in the right-hand side of (4) can be rewritten as

$$\begin{aligned} &\sum_{c \in F_{2^e}^*} \sum_{d \in F_{2^e}^*} M_\delta(cd,d) \sum_{x_1 \in F_{2^e}^*} (-1)^{f(x_1cd)+g(x_1d)} \\ &= \sum_{c \in F_{2^e}^*} \sum_{d \in F_{2^e}^*} M_\delta(cd,d) \sum_{x_1 \in F_{2^e}^*} (-1)^{f(x_1c)+g(x_1)} \\ &= 2^{n-2e} \sum_{c \in F_{2^e}^*} \sum_{x_1 \in F_{2^e}^*} (-1)^{f(x_1c)+g(x_1)} \\ &= 2^{n-2e} \left(\sum_{x_1 \in F_{2^e}^*} (-1)^{g(x_1)} \right) \left(\sum_{c \in F_{2^e}^*} (-1)^{f(c)} \right) \\ &= 2^{n-2e} I(f) I(g). \end{aligned}$$

Therefore, we have

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

□

III. A New binary LCZ sequence set

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

Lemma 4 ([5]): Let e be an integer such that 2^e-1 is a prime. Let $s(t)$ be a Legendre sequence defined in (1). Then $s(t)$ can be represented as follows

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

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

Theorem 5: Let $e>3$ be an integer such that $2^e-1=p\equiv 3 \pmod 4$ is a prime. Let $s(t)$ be a Legendre sequence of period 2^e-1 defined in (1). Then there is no integer pair (a,b) that satisfies the relation

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

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 of F_{2^e}. The above equation implies that for every λ such that $S(\lambda)\neq 0$, α^λ is the solution of $1+z^a+z^b=0$.

From Lemma 4 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

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

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 6: Let $e>3$ be an integer such that $2^e-1=p\equiv 3 \pmod 4$ is a prime. Let $s(t)$ be a Legendre sequence of period 2^e-1 defined in (1). 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 5, 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

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

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 3, Theorem 5, and Theorem 6, we can construct binary LCZ sequence with parameters $(2^n-1,2^{e-1},(2^n-1)/(2^e-1),1)$ as in the following theorem.

Theorem 7: Let n and e be integers such that $e|n$ and 2^e-1 is a prime and $T=(2^n-1)/(2^e-1)$. Let α be a primitive element of F_{2^n} and $\beta=\alpha^T$ be a primitive element of F_{2^e}. Let $l(\beta^t)=s(t)$ be the Legendre sequence defined in (1) of period 2^e-1 and the function $h(x)$ from F_{2^n} to F_{2^m} be a 1-form function over F_{2^e} with balance and difference balance property. Then the sequence set $\mathcal{S}$ defined by

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

where $f_i(t)$ is given as

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

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

Proof: From Theorem 5 and Theorem 6, 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

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

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

From Theorem 3 and (8), $R_{i,j}(\tau) = R_{a,b}(\delta)$ can be rewritten as

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

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 have the low correlation zone $[1-T, T-1]$.

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

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

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

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 have low correlation zone $[1-T, T-1]$.

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

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

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

From the above equation, it is straightforward that f_i and f_j have 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

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

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

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] S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *preprint*, 2004.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.