New Construction of Perfect Sequence Set and Low Correlation Zone Sequence Set ⋆

Hai Xiong, Longjiang Qu, and Chao Li

Department of Mathematics and System Science, Science College, National University of Defence Technology, Changsha, China 410073
xiong.hai@163.com,ljqu_happy@hotmail.com,lichao_nudt@sina.com

Abstract. For a given binary ideal autocorrelation sequence, we construct a perfect sequence set by changing a few bits of the sequence. The set has a large size with respect to the period of its sequences. Based on the constructed perfect sequence set, a new class of low correlation zone sequence sets whose low correlation zone length can be chosen flexibly are obtained. Moreover, the new constructed low correlation zone sequence sets can attain Tang-Fan-Matsufuji's bound with suitably chosen parameters.

Index Terms—Perfect sequence set, Almost perfect sequence set, LCZ sequence set

1 Introduction

Sequences with good properties of autocorrelation and cross-correlation are widely used in the engineering application such as CDMA systems. Constructing sequence sets with desirable properties is very important.

Low correlation zone(LCZ) sequences are useful in approximately synchronized CDMA systems. There are many approaches[1-5] for constructing LCZ sequence sets. Unfortunately, in the most known constructions, except for Kim and Zhou's works[3, ?], the length of the LCZ can not be flexibly chosen. In this paper, we give a new method to construct the LCZ sequence set whose length of the LCZ can be chosen freely. Besides, some of new constructed LCZ sequence sets can attain Tang-Fan-Matsufuji's bound[6].

Recently, Cai et al.[7] presented some new concepts called the almost perfect sequence set(APSS) and the perfect sequence set(PSS). A set is called an APSS if it has both low autocorrelation magnitudes and cross-correlation magnitudes except for a few exceptional shifts, and when there is only one exceptional shift, the set is called a PSS. In paper [7], the APSSs are used to construct the LCZ sequence sets. However, their method to construct APSSs is based on the assumption of the existence of the PSS. Although some PSSs have been constructed by them, all of these PSSs share a weakness that their size is quite small. They proposed some problems, one of which is how to efficiently construct the PSS with large size. In this paper, we obtain a new family of PSSs with large size by modifying a few bits of the ideal two-level autocorrelation sequences. As far as we known, it is the first construction of a family of PSSs with large size in the literature.

The ideal autocorrelation sequences have good properties, and they are usually used to construct the other sequences. For a given binary ideal autocorrelation sequence, we find that the set comprised of the sequences which are constructed by modifying a few bits of the ideal autocorrelation sequence is a PSS. Moreover, the PSS has a large size. Based on the constructed PSS, we obtain a new class of LCZ sequence sets by shifting technology. The low correlation zone length of the sets can be chosen flexibly, and some of the sets are optimal with respect to Tang-Fan-Matsufuji's bound. Without loss of generality, we will just

⋆ The work was supported by the Natural Science Foundation of China (No:60803156, No:61070215)

discuss how to construct the PSSs and the LCZ sequence sets based on the binary ideal autocorrelation sequences with period $N(\equiv -1 \mod 4)$.

The following paper is organized as follows. In section II, we introduce some basic notions. In section III, we give a new method to construct the PSS by modifying a few bits of a binary ideal autocorrelation sequence. In section IV, a new class of LCZ sequence sets which are optimal with respect to Tang-Fan-Matsufuji's bound are obtained based on the constructed PSS. Finally we conclude this paper in section V.

2 Preliminaries

In this section, we review some basic notions. Binary ideal autocorrelation sequences are the foundation of this paper, and we will give a detailed introduction.

2.1 Correlation

The cross-correlation function of two binary periodic sequences $u = (u_0, u_1, \cdots, u_{N-1})$ and $v = (v_0, v_1, \cdots, v_{N-1})$ is defined by

$$C_{u,v}(\tau) = \sum_{i=0}^{N-1} (-1)^{u_i + v_{i+\tau}},$$

where $u_i, v_i \in \{0, 1\}$ and $\tau \in \mathbb{Z}_N$. If the sequences u and v are identical, then it is called the autocorrelation function of sequence u, and we denote it by $C_u(\tau)$.

2.2 Binary ideal autocorrelation sequence

A binary sequence u with period $N(\equiv -1 \mod 4)$ is called an ideal two-level autocorrelation sequence if the autocorrelation function of u satisfies

$$C_u(\tau) = \begin{cases} N, & \text{if} \quad \tau = 0; \\ -1, & \text{if} \quad \tau \neq 0. \end{cases}$$

There are many examples of binary ideal two-level autocorrelation sequences such as m sequences, Legendre sequences, Hall's sextic residue sequences[8], Kasami power function sequences[9], Welch-Gong(WG) sequences[10], GMW sequences[11], hyperoval sequences[12] et al..

Legendre Sequence: Let $p = 4t - 1$ be a prime. The sequence $s = (s_0, s_1, \cdots, s_{p-1})$ is called Legendre sequence if

$$s_i = \begin{cases} 0, & \text{if } i \equiv x^2 \mod p \text{ for some } x \neq 0; \\ 1, & \text{otherwise.} \end{cases}$$

Sextic residue sequence: Let $p = 4t-1 = 4a^2+27$ be a prime, u be a primitive element of $\mathbb{Z}_p$, and let $G = \{a \in \mathbb{Z}_p^* | x^6 \equiv a \mod p, x \in \mathbb{Z}_p^*\}$. The sequence $s = (s_0, s_1, \cdots, s_{p-1})$ is called Hall's sextic residue sequence if

$$s_i = \begin{cases} 0, & \text{if } i \in G \cup u^3 G \cup u^{i_0} G; \\ 1, & \text{otherwise,} \end{cases}$$

where $u^{i_0}G$ is the coset containing 3.

Kasami power function sequence: Let k be an integer satisfying $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$ and $\gcd(k,n) = 1$. For $d = 4^k - 2^k + 1$, consider a set $B_k = \{(x+1)^d + x^d + 1|\ x \in \mathbb{F}_{2^n}\}$. The sequence $s = (s_0, s_1, \cdots, s_{2^n-1})$ is called Kasami power function sequence if

$$s_i = \begin{cases} 0, & \text{if } \alpha^i \in B_k; \\ 1, & \text{otherwise,} \end{cases}$$

where α is a primitive element of $\mathbb{F}_{2^n}$.

WG sequence: Let $n = 3k \pm 1$, $d = 2^{2k} - 2^k + 1$, and let $\delta_k(x) = (x+1)^d + x^d$ be a map on $\mathbb{F}_{2^n}$. Consider a set

$$W_k = \begin{cases} \{\delta_k(x)|x \in \mathbb{F}_{2^n}\}, & \text{if } n \text{ is even;} \\ \mathbb{F}_{2^n} - \{\delta_k(x)|x \in \mathbb{F}_{2^n}\}, & \text{if } n \text{ is old.} \end{cases}$$

Then, the sequence $s = (s_0, s_1, \cdots, s_{2^n-1})$ is called WG sequence if

$$s_i = \begin{cases} 0, & \text{if } \alpha^i \in W_k; \\ 1, & \text{if } \alpha^i \notin W_k, \end{cases}$$

where α is a primitive element of $\mathbb{F}_{2^n}$.

GMW sequence: Let α be a primitive element of $\mathbb{F}_{2^n}$, $m|n$, and $g(x)$ be an orthogonal function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Then the sequence $s = (s_0, s_1, \cdots, s_{2^n-1})$ is called GMW sequence if $s_i = f(\alpha^i)$, where $f(x)$ is a composition of $Tr_m^n(x^k)$ and $g(x)$, $f(x) = g(x) \circ Tr_m^n(x^k)$, $\gcd(k, 2^n - 1) = 1$. $Tr_m^n(x)$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, and it is defined by $Tr_m^n(x) = \sum_{k=0}^{n/m-1} x^{2^{mk}}$.

Hyperoval sequence: Let n be an odd integer, consider a set $M_k = \{x + x^k|x \in \mathbb{F}_2\}$, where k is given as follows:
(1) Singer type: $k = 2$, Segre type: $k = 6$;
(2) Glynn type I: $k = 2^\sigma + 2^\tau$ where $\sigma = \frac{n+1}{2}$ and $4\tau \equiv 1 \mod n$;
(3) Glynn type II: $k = 3 \cdot 2^\sigma + 4$ with $\sigma = \frac{n+1}{2}$.
Then, the sequence $s = (s_0, s_1, \cdots, s_{2^n-1})$ is called hyperoval sequence if

$$s_i = \begin{cases} 0, & \text{if } \alpha^i \in M_k; \\ 1, & \text{if } \alpha^i \notin M_k, \end{cases}$$

where α is a primitive element of $\mathbb{F}_{2^n}$.

2.3 PSS and LCZ sequence set

APSS and PSS. A sequence set V is called an (N, K, c, m)-almost perfect sequence set(APSS), if V contains K shift-distinct sequences of period N and satisfies the following two conditions:
(1) For each $u \in V$ and each $1 \leq \tau \leq N - 1$, $|C_u(\tau)| \leq c$ except for at most $(m-1)$ $\tau's$;
(2) For each $u \neq v \in V$ and each $0 \leq \tau \leq N - 1$, $|C_{u,v}(\tau)| \leq c$ except for at most m $\tau's$.
Moreover, when $m = 1$, V is called an (N, K, c)-perfect sequence set(PSS).

LCZ sequence set. A sequence set V is called an (N, M, L, δ)-low correlation zone(LCZ) sequence set, if V contains M shift-distinct sequences of period N and satisfies the following two conditions:

(1) For each $u \in V$ and each $0 < |\tau| \le L$, $|C_u(\tau)| \le \delta$;
(2) For each $u \ne v \in V$ and each $|\tau| \le L$, $|C_{u,v}(\tau)| \le \delta$.

For two subsets of $\mathbb{Z}_N$, A and B, let $A \triangle B$ denote $(A \cup B) - (A \cap B)$, and $A \pm \tau = \{x \pm \tau \ |x \in A\}$.

3 Construction of perfect sequence set

The PSS is a new concept proposed by Cai et al.[7]. They have constructed some PSSs, but all of these sets have a small size. As our best known, there are no other people have researched this problem. In this section, we construct a PSS by changing a few bits of an ideal two-level autocorrelation sequence. And the size of the PSS may be quite large.

Lemma 1. *Let $N \equiv -1 \mod 4$, $r < \frac{N+1}{4}$ be a positive integer and $s = (s_0, s_1, \cdots, s_{N-1})$ be a binary ideal two-level autocorrelation sequence with period N. Consider a set $V_s^r = \{s^B \ |B \subset \mathbb{Z}_N,\ |B| \le r\}$, where the sequence $s^B = (s_0^B, s_1^B, \cdots, s_{N-1}^B)$ is defined by*

$$s_i^B = \begin{cases} s_i + 1, & \text{if} \quad i \in B; \\ s_i, & \text{if} \quad i \notin B. \end{cases}$$

Then these sequences in V_s^r are shift-distinct, and $|V_s^r| = \sum_{k=0}^{r} C_N^k$. Moreover, for any two different sequences s^{B_1} and s^{B_2}, $|C_{s^{B_1},s^{B_2}}(\tau)| \le 4r+1$ holds for any $\tau \ne 0$.

Proof. For each two different sequences s^{B_1}, s^{B_2}, they are shift-distinct if and only if for each τ, their cross-correlation $C_{s^{B_1},s^{B_2}}(\tau) \ne N$. For a given τ, let A_1, A_2, A_3, A_4 denote $\mathbb{Z}_N - (B_1 \cup (B_2 - \tau))$, $B_1 \cap (B_2 - \tau)$, $B_1 - (B_2 - \tau)$, $(B_2 - \tau) - B_1$ respectively. Then we have the following result

$$\begin{aligned} C_{s^{B_1},s^{B_2}}(\tau) =& \sum_{i\in\mathbb{Z}_N} (-1)^{s_i^{B_1} + s_{i+\tau}^{B_2}} \\ =& \sum_{i\in A_1} (-1)^{s_i^{B_1} + s_{i+\tau}^{B_2}} + \sum_{i\in A_2} (-1)^{s_i^{B_1} + s_{i+\tau}^{B_2}} \\ &+ \sum_{i\in A_3} (-1)^{s_i^{B_1} + s_{i+\tau}^{B_2}} + \sum_{i\in A_4} (-1)^{s_i^{B_1} + s_{i+\tau}^{B_2}} \\ =& \sum_{i\in A_1} (-1)^{s_i + s_{i+\tau}} + \sum_{i\in A_2} (-1)^{s_i + s_{i+\tau}} \\ &+ \sum_{i\in A_3} (-1)^{s_i + s_{i+\tau}+1} + \sum_{i\in A_4} (-1)^{s_i + s_{i+\tau}+1} \\ =& \sum_{i\in\mathbb{Z}_N} (-1)^{s_i + s_{i+\tau}} - 2\sum_{i\in A_3} (-1)^{s_i + s_{i+\tau}} - 2\sum_{i\in A_4} (-1)^{s_i + s_{i+\tau}} \\ =& C_s(\tau) - 2 \sum_{i\in B_1 \triangle (B_2 - \tau)} (-1)^{s_i + s_{i+\tau}}. \end{aligned} \tag{1}$$

If $\tau = 0$, then $C_{s^{B_1},s^{B_2}}(0) = N - 2|B_1 \triangle B_2| \le N-2$; if $\tau \ne 0$, then $-(1+4r) \le C_{s^{B_1},s^{B_2}}(\tau) \le 4r-1$. So all the sequences in V_s^r are shift-distinct, and $|C_{s^{B_1},s^{B_2}}(\tau)| \le 4r+1$ holds for any $\tau \ne 0$.

It is clear that $|V_s^r| = \sum_{k=0}^{r} C_N^k$.

By the above discussion, the lemma is proved.

Lemma 2. *Let V_s^r be the sequence set defined in the Lemma 1, $s^B \in V_s^r, \tau \neq 0$. Then*

$$C_{s^B}(\tau) \in \{-2|B \triangle (B-\tau)| - 1 + 4t \ : \ 0 \leq t \leq |B \triangle (B-\tau)|\}.$$

And clearly, $|C_{s^B}(\tau)| \leq 4r+1$ holds when $\tau \neq 0$.

Proof. Following a similar way in Lemma 1, we can get that

$$C_{s^B}(\tau) = C_s(\tau) - 2 \sum_{i \in B \triangle (B-\tau)} (-1)^{s_i + s_{i+\tau}}. \tag{2}$$

Note that s is an ideal two-level autocorrelation sequence, the lemma is proved.

Theorem 1. *Let V_s^r be the sequence set defined in Lemma 1. Then V_s^r is an $(N, \sum_{k=0}^{r} C_N^k, 4r+1)$-PSS.*

Proof. According to Lemma 1 and Lemma 2, we can get that for each $s^{B_1}, s^{B_2} \in V_s^r$, and for each $1 \leq \tau \leq N-1$, $|C_{s^{B_1}, s^{B_2}}(\tau)| \leq 4r+1$. So the theorem is proved.

Theorem 2. *For any positive integer $n \geq 3$, there exists a $(2^n-1, 2^n, 5)$-PSS; for any prime integer $p = 4t-1$, there exists a $(p, p+1, 5)$-PSS.*

Proof. For any positive integer $n \geq 3$, let s be an m sequence or Kasami power function sequence with period (2^n-1), and $r = 1$. According to Theorem 1, we can obtain a $(2^n-1, 2^n, 5)$-PSS. For any prime integer $p = 4t-1$, let s be a Legendre sequence with period p, and $r = 1$. According to Theorem 1, we can obtain a $(p, p+1, 5)$-PSS.

Remark 1. Cai et al.[7] constructed some PSSs such as $(p, 2, 3)$-PSS and $(p, 4, 3)$-PSS. They also discussed the sequence sets in the literatures[3][4] which can be considered as PSSs or APSSs. However, all of these PSSs have a small size with respect to the period of the sequences. According to Theorem 2, the size of the PSS constructed in our paper is large.

As an example, we give a $(31, 32, 5)$-PSS based on an m sequence with period 31.

Example 1. Let $s = (1111100110100100001010111011000)$ be an m sequence with period 31 and $r = 1$, then the V_s^1 defined in Lemma 1 is

$$\begin{aligned}
\{&(1111100110100100001010111011000), (\mathbf{0}111100110100100001010111011000),\\
&(1\mathbf{0}11100110100100001010111011000), (11\mathbf{0}1100110100100001010111011000),\\
&(111\mathbf{0}100110100100001010111011000), (1111\mathbf{0}00110100100001010111011000),\\
&(11111\mathbf{1}0110100100001010111011000), (111110\mathbf{1}110100100001010111011000),\\
&(1111100\mathbf{0}10100100001010111011000), (11111001\mathbf{0}0100100001010111011000),\\
&(111110011\mathbf{1}100100001010111011000), (1111100110\mathbf{0}00100001010111011000),\\
&(11111001101\mathbf{1}0100001010111011000), (111110011010\mathbf{1}100001010111011000),\\
&(1111100110100\mathbf{0}00001010111011000), (11111001101001\mathbf{1}0001010111011000),\\
&(111110011010010\mathbf{1}001010111011000), (1111100110100100\mathbf{1}01010111011000),\\
&(11111001101001000\mathbf{1}1010111011000), (111110011010010000\mathbf{0}010111011000),\\
&(1111100110100100001\mathbf{1}10111011000), (11111001101001000010\mathbf{0}0111011000),\\
&(111110011010010000101\mathbf{1}111011000), (1111100110100100001010\mathbf{0}11011000),\\
&(11111001101001000010101\mathbf{0}1011000), (111110011010010000101011\mathbf{0}011000),\\
&(1111100110100100001010111\mathbf{1}11000), (11111001101001000010101110\mathbf{0}1000),\\
&(111110011010010000101011101\mathbf{0}000), (1111100110100100001010111011\mathbf{1}00),\\
&(11111001101001000010101110110\mathbf{1}0), (111110011010010000101011101100\mathbf{1})\}.
\end{aligned}$$

Let $M_\mu = \left|\{(\{s^{B_1}, s^{B_2}\}, \tau) \mid C_{s^{B_1}, s^{B_2}}(\tau) = \mu\}\right|$, where $s^{B_1}, s^{B_2} \in V_s^r, \tau \in \mathbb{Z}_N$. The distribution of correlation of the $(31, 32, 5)$-PSS is given in Table 1.

Table 1. Distribution of correlation of the $(31, 32, 5)$-PSS

μ	-5	-3	-1	1	3	27	29	31
M_μ	3255	450	7935	480	3720	465	31	32

Remark 2. As shown in Table 1, $M_{31} = 32$ proves that all the sequences in $(31, 32, 5)$-PSS are shift-distinct.

Let s^i denote the $(i+1)$th sequence in V_s^1 as shown in Example 1. Let $M_{s^i,s^j}(\mu) = |\{\tau | C_{s^i,s^j}(\tau) = \mu, \tau \in \mathbb{Z}_N\}|$. The distributions of correlation of some pairs of sequences in V_s^1 are given in Table 2.

Table 2. Distribution of correlation of some pairs of sequences in V_s^1

μ	-5	-3	-1	1	3	27	29	31
$M_{s^0,s^1}(\mu)$	0	15	0	15	0	0	1	0
$M_{s^0,s^6}(\mu)$	0	14	0	16	0	0	1	0
$M_{s^2,s^3}(\mu)$	8	0	13	0	9	1	0	0
$M_{s^4,s^4}(\mu)$	6	0	18	0	6	0	0	1
$M_{s^7,s^7}(\mu)$	4	0	20	0	6	0	0	1

4 Construction of low correlation zone sequence set

In this section, we construct a new family of LCZ sequence sets based on the constructed PSS. In our construction, the length of the low correlation zone can be chosen flexibly. Besides, some of the sets can attain Tang-Fan-Matsufuji's bound.

For a given ideal autocorrelation sequence s, let V_s^r be a sequence set defined in Lemma 1, T denote the left shift operation such that $Ts = (s_1, \cdots, s_{N-1}, s_0)$, $L \leq [\frac{N}{2}]$ can be chosen flexibly and $M = [\frac{N}{L}]$. We can construct an $(N, M, L-1, 4r+1)$-LCZ sequence set based on the set V_s^r.

Theorem 3. *Given arbitrary M different sequences $s^{B_0}, \cdots, s^{B_{M-1}} \in V_s^r$, let $W = \{s^0, \cdots, s^{M-1}\}$ be a sequence set, where $s^i = T^{iL}s^{B_i}$. Then W is an $(N, M, L-1, 4r+1)$-LCZ sequence set.*

Proof. Given arbitrary sequence $s^i, s^j \in W$ and $|\tau| \leq L-1$, we have

$$\begin{aligned} C_{s^i,s^j}(\tau) &= C_{T^{iL}s^{B_i},T^{jL}s^{B_j}}(\tau) \\ &= C_{s^{B_i},s^{B_j}}(\tau + (j-i)L). \end{aligned} \tag{3}$$

Note that $0 \leq i, j \leq M-1$ and $|\tau| \leq L-1$, so $|\tau + (j-i)L| \leq ML - 1 < N$. And $|\tau + (j-i)L| = 0$ if and only if $\tau = 0, i = j$. By the above discussion, with Lemma 1 and Lemma 2, we can get the following results:
(1) For each $s^i \in W$ and each $0 < |\tau| \leq L-1$, $|C_{s^i}(\tau)| \leq 4r+1$.
(2) For each $s^i, s^j \in W (i \neq j)$ and each $|\tau| \leq L-1$, $|C_{s^i,s^j}(\tau)| \leq 4r+1$.
So the theorem is proved.

Tang Xiaohu et al.[6] have presented an upper bound on the size of the LCZ sequence set. Their result is equivalent to the following lemma.

Lemma 3. *(X.H. Tang, P.Z. Fan and S. Matsufuji) Let V be an (N, M, L, c)-LCZ sequence set. Then*

$$M \leq \frac{N^2 - c^2}{(N - c^2)L}. \tag{4}$$

Theorem 4. *Let $N \geq 15^3, L \geq N^{\frac{2}{3}}, L|N, r \leq \frac{N^{\frac{1}{3}}-3}{12}$. Then the $(N, M, L-1, 4r+1)$-LCZ sequence set constructed in Theorem 3 is optimal with respect to Tang-Fan-Matsufuji's bound.*

Proof. Let M_o denote the Tang-Fan-Matsufuji's bound. According to Lemma 3, we have

$$\begin{aligned} M_o \leq &\frac{N^2 - (4r+1)^2}{(N - (4r+1)^2)(L-1)} = \frac{N - 4r - 1}{N - (4r+1)^2} \frac{N + 4r + 1}{L - 1} \\ = &\frac{N}{L} \frac{N - 4r - 1}{N - (4r+1)^2} \frac{N + 4r + 1}{N} \frac{L}{L-1} \\ < &\frac{N}{L} \frac{N}{N - (4r+1)^2} \frac{N + 4r + 1}{N} \frac{L}{L-1} \end{aligned}$$

$$\begin{aligned}
&\leq \frac{N}{L}\Big(1+\frac{(4r+1)^2}{N-(4r+1)^2}\Big)\Big(1+\frac{4r+1}{N}\Big)\Big(1+\frac{1}{L-1}\Big)\\
&\leq \frac{N}{L}\Big(1+\frac{2(4r+1)^2}{N}\Big)\Big(1+\frac{4r+1}{N}\Big)\Big(1+\frac{2}{L}\Big)\\
&\leq \frac{N}{L}\Big(1+\frac{2(4r+1)^2}{N}+\frac{2}{L}\Big(1+\frac{2(4r+1)^2}{N}\Big)\\
&\quad+\frac{4r+1}{N}\Big(1+\frac{2(4r+1)^2}{N}+\frac{2}{L}+\frac{2(4r+1)^2}{N}\frac{2}{L}\Big)\Big)\\
&\leq \frac{N}{L}\Big(1+\frac{2(4r+1)^2}{N}+\frac{3}{L}+\frac{2(4r+1)}{N}\Big)\\
&\leq \frac{N}{L}(1+\frac{1}{N^{\frac{1}{3}}})\leq \frac{N}{L}+1.
\end{aligned} \tag{5}$$

So $M_o = \left[\frac{N}{L}\right] = M$. The theorem is proved.

Theorem 5. *For any positive integer $m > 3$, let $N = 2^{3m} - 1$, $L = 2^{2m} + 2^m + 1$ and $r \leq 2^{m-4}$. Then we can construct an $(N, 2^m - 1, L - 1, 4r + 1)$-LCZ sequence set which is optimal with respect to Tang-Fan-Matsufuji's bound.*

Proof. For any positive integer $m > 3$, let s be an m sequence with period $2^{3m}-1$. According to Theorem 1, we can obtain an $(N, \sum_{k=0}^{r} C_N^k, 4r + 1)$-PSS, where $N = 2^{3m} - 1$. According to Theorem 3, based on the PSS, we can construct an $(N, M, L-1, 4r+1)$-LCZ sequence set, where $M = 2^m - 1$, $L = 2^{2m} + 2^m + 1$ and $r \leq 2^{m-4}$. It is easy to check that the parameters N, L, M and r satisfy the properties of Theorem 4. So the $(N, M, L-1, 4r+1)$-LCZ sequence set is optimal with respect to Tang-Fan-Matsufuji's bound.

We compute the sizes of some $(N, M, L - 1, 5)$-LCZ sequence sets which are constructed based on m sequences. Even for $N < 15^3$, there are also many $(N, M, L-1, 5)$-LCZ sequence sets which are optimal or almost optimal with respect to Tang-Fan-Matsufuji's bound. Some results are given in Table 3.

5 Conclusion

In this paper, we present a new method for constructing the PSS and the LCZ sequence set. For a given binary ideal two-level autocorrelation sequence with period N, we obtain an $(N, \sum_{k=0}^{r} C_N^k, 4r + 1)$-PSS comprised of the sequences which are constructed by modifying a few bits (no more than r) of the ideal autocorrelation sequence. Based on the PSS, a new class of $(N, M, L - 1, 4r + 1)$-LCZ sequence sets are constructed, where L can be chosen flexibly and $M = [\frac{N}{L}]$. Besides, the new constructed PSSs have a large size and the LCZ sequence sets can attain Tang-Fan-Matsufuji's bound with suitable parameters.

We just discuss constructing PSSs and LCZ sequence sets based on the binary ideal two-level autocorrelation sequences with period $N(\equiv -1 \mod 4)$. However, the method can be generalized easily along the following two directions. On one hand, one can construct PSSs and LCZ sequence sets based on binary ideal autocorrelation sequences with other types period. On the other hand, one can similarly construct p-ary PSSs and LCZ sequence sets once the p-ary ideal two-level autocorrelation sequences are provided.

References

1. Tang X H, Fan P Z. A Class of Pseudonoise Sequence over GF(P) with Low Correlation Zone. IEEE Trans Inf Theory, 2001, 47: 1644-1649

Table 3. A comparison of the size of LCZ-sequence sets constructed in our paper and Tang-Fan-Matsufuji's bound

Sequence Length	LCZ Length	Our Size	Optimal Bound
511	25	19	21
511	26	18	20
511	27	18	19
511	50	10	10
511	100	5	5
511	101	5	5
511	102	4	5
1023	35	28	29
1023	45	22	23
1023	55	18	19
1023	62	16	16
1023	100	10	10
1023	101	10	10
1023	102	9	10
2047	60	33	34
2047	70	28	29
2047	80	25	25
2047	90	22	23
2047	200	10	10
2047	201	10	10
2047	204	9	10
4095	100	40	41
4095	200	20	20
4095	300	13	13
4095	400	10	10
4095	409	9	10
4095	500	8	8
4095	600	6	6

2. Kim S H, Jang J W, No J S, Chung H. New Constuction of Quaternary Low Correlation Zone Sequence. IEEE Trans Inf Theory, 2005, 51: 1469-1477

3. Kim Y S, Jang J W, No J S, Chung H. New Design of Low-Correlation Zone Sequence Sets. IEEE Trans Inf Theory, 2006, 52: 4607-4616

4. Gong G, Golomb S W, Song H Y. A Note on Low-Correlation Zone Signal Sets. IEEE Trans Inf Theory, 2007, 53: 2575-2581

5. Zhou Z C, Tang X H, Gong G. A New Class of Sequences with Zero or Low Correlation Zone Based on Interleaving Technique. IEEE Trans Inf Theory, 2008, 54: 4267-4273

6. Tang X H, Fan P Z, Matsufuji S. Lower Bounds on Correlation of Spreading Sequence Set with Low or Zero Correlation Zone. Electron Lett, 2000, 36: 551-552

7. Cai K, Weng G B, Cheng X Q. Binary Almost-Perfect Sequence Sets. IEEE Trans Inf Theory, 2010, 56: 3594-3604

8. Golomb S W, Gong G. Signal Design for Good Correlation. New York: Cambridge University Press, 2005

9. Dillon J F, Dobbertin H. New Cyclic Difference Sets with Singer Parameters. Finite Fields and Their Applications, 2004, 10: 342-389

10. No J S, Golomb S W, Gong G, Lee H K, Gall P. Binary Pseudorandom Sequences of Period $2^m - 1$ with Ideal Autocorrelation. IEEE Trans Inf Theory, 1998, 44: 814-817

11. Gardon B, Mills W H, Welch L R. Some New Difference Sets. Canadian J Math, 1962, 14: 614-625

12. Maschietti A. Difference Sets and Hyperovals. Designs Codes and Cryptopgraphy, 1998, 14: 89-98