Construction of multiple quasi-complementary sequence sets with low inter-set cross-correlation

Yushu Tian Tao Liu Xiuping Peng Yubo Li

School of Information Science and Engineering
Hebei Key Laboratory of Information Transmission and Signal Processing
Yanshan University
Qinhuangdao, China

tianyushu@stumail.ysu.edu.cn {liutaotao,pengxp,liyubo6316}@ysu.edu.cn

Abstract

Recently, quasi-complementary sequence sets (QCSSs) have attracted interests for supporting large number of users in multi-carrier code-division multiple-access (MC-CDMA) systems. In applications, QCSSs that possess large set size and low correlation properties are desired. This work has two main contributions. Firstly, we present a method for generating multiple asymptotically optimal aperiodic low correlation complementary sequence sets (LC-CSSs) with low inter-set cross-correlation. Secondly, the combination of proposed LC-CSSs can result in a large-capacity aperiodic LC-CSS.

1 Introduction

Mutually orthogonal complementary sequence sets (MOCSSs) [1] have found extensive applications in communication systems owing to their ideal correlation properties, particularly in the design of radar system waveforms [2], channel estimation [3], etc. It is well known, the disadvantage of MOCSSs is that the set size cannot exceed the flock size (the number of constituent sequences) [4], which will limit the applications of complementary sets in multi-carrier code-division multiple-access (MC-CDMA) systems with large users to support.

To address this issue, the concept of quasi-complementary sequence set (QCSS), of which low correlation complementary sequence set (LC-CSS) is one subtype, was initially introduced by Liu *et al.* in [5]. One can extend communication capacity and reduce interference by utilizing QCSSs in communications [6]. Numerous studies have been carried

Corresponding author: Tao Liu.

This work was supported in part by the National Natural Science Foundation of China under Grant 62241110, in part by the Central government guides local science and technology development Foundation under Grant 236Z0403G.

out in order to design periodic and aperiodic QCSSs. In 2013, Liu *et al.* [5] proposed periodic QCSSs over the Singer difference set. Furthermore, Li *et al.* [7] constructed periodic QCSSs based on almost difference sets. In [8], Luo *et al.* constructed three classes of periodic small-alphabet sizes QCSSs. Aperiodic QCSSs have the same important applications in communication systems. Design of aperiodic QCSSs with various parameters is an interesting problem. Li *et al.* [9] proposed three classes of aperiodic LC-CSSs and one class of low correlation zone complementary sequence sets (LCZ-CSSs). Later, Zhou *et al.* [10] constructed QCSSs with new asymptotically optimal parameters. Authors in [11] constructed aperiodic QCSSs with larger set size from Florentine rectangles. In [12], aperiodic QCSSs of length $p_1^{m_1} p_2^{m_2}$ were constructed by using multivariate functions. Recently, the concept of QCSS was extended to two dimension (2-D) and the theoretical bounds of 2-D quasi-complementary array sets was presented in [13].

On the other hand, to reduce inter-cell interference in multi-cell scene, multiple sequence sets possessing favorable inter-set correlation properties are needed. Multiple optimal zero correlation zone (ZCZ) sequence sets with good cross-correlation between the different sets were introduced in [14]. Liu *et al.* [15] constructed aperiodic LC-CSSs combining several sets of complete complementary codes (CCCs) in 2019. Very recently, the authors in [16] have derived a new correlation lower bound for QCSSs composed of several CCCs, and they presented a construction of such QCSSs with flexible-alphabet sizes, which are convenient for practical applications.

As far as the authors are aware, the design of large-capacity LC-CSSs with multiple subsets has yet been introduced in other literature. This is the primary motivation of this paper. In this paper, we construct multiple aperiodic (p^2, p, p, p)-LC-CSSs, achieving the theoretical bound of LC-CSSs presented in [17]. Furthermore, we propose a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS by combining these LC-CSSs.

This paper is structured as follows for the remainder. Fundamental definitions are presented in Sect. 2. In Set. 3, we present the construction of multiple aperiodic LC-CSSs. Furthermore, a large-capacity aperiodic LC-CSS is generated through the combination of these LC-CSSs into a new set. Lastly, the paper is summarized in Sect. 4.

2 Preliminaries

Let $\mathbf{c} = (c_0, c_1, \cdots, c_{N-1})$ and $\mathbf{d} = (d_0, d_1, \cdots, d_{N-1})$ denote two length-N complex-valued sequences. The aperiodic correlation between $\mathbf{c}$ and $\mathbf{d}$ at time-shift τ is defined as

$$\widetilde{R}_{\mathbf{c},\mathbf{d}}(\tau) = \begin{cases} \sum_{t=0}^{N-1-\tau} c_t d_{t+\tau}^*, & 0 \le \tau \le N-1 \\ \sum_{t=0}^{N-1+\tau} c_{t-\tau} d_t^*, & 1-N \le \tau \le -1 \\ 0, & |\tau| \ge N, \end{cases} \tag{1}$$

where d_t^* denotes the complex conjugation of d_t.

Consider $\mathcal{S} = \{\mathbf{S}^0, \mathbf{S}^1, \cdots, \mathbf{S}^{K-1}\}$, having K sequence sets, each sequence set $\mathbf{S}^k$ comprises M length-N sequences, i.e., $\mathbf{S}^k = \{\mathbf{s}_0^k, \mathbf{s}_1^k, \cdots, \mathbf{s}_{M-1}^k\}$, $\mathbf{s}_m^k = \left(s_{m,0}^k, s_{m,1}^k, \cdots, s_{m,N-1}^k\right)$, $0 \le k \le K-1$, $0 \le m \le M-1$. The sequence set can be written in a matrix form with size $M \times N$, i.e.,

$$\mathbf{S}^k = \begin{bmatrix} s^k_{0,0}, & s^k_{0,1}, & \cdots & s^k_{0,N-1} \\ s^k_{1,0}, & s^k_{1,1}, & \cdots & s^k_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ s^k_{M-1,0}, & s^k_{M-1,1}, & \cdots & s^k_{M-1,N-1} \end{bmatrix}. \tag{2}$$

The set $\mathcal{S}$ is called a $(K, M, N, \delta_{\max})$-QCSS if for any $\mathbf{S}^{k_1}, \mathbf{S}^{k_2} \in \mathcal{S}$, where $0 \leq k_1, k_2 \leq K-1$, we have

$$\left|\widetilde{R}_{\mathbf{S}^{k_1},\mathbf{S}^{k_2}}(\tau)\right| = \left|\sum_{m=0}^{M-1} \widetilde{R}_{\mathbf{s}^{k_1}_m,\mathbf{s}^{k_2}_m}(\tau)\right| \leq \delta_{\max}, \tag{3}$$

for $k_1 \neq k_2, 0 \leq \tau \leq N-1$ or $k_1 = k_2, 0 < \tau \leq N-1$. Notably, K, M, N, and $\delta_{\max}$ represent the set size, the flock size, the length of each constituent sequence, and the maximum aperiodic correlation magnitude, respectively. QCSSs are divided into two types: LC-CSS and LCZ-CSS. An LCZ-CSS represents a set of two-dimensional matrices whose correlation magnitudes are non-zero but relatively low for the non-trivial time-shifts within a low correlation zone (LCZ). An LC-CSS is produced when the length of the LCZ is equivalent to the length of each constituent sequence. Specially, when $\delta_{\max} = 0$, the QCSS reduce to (K, M, N)-MOCSS. If $\delta_{\max} = 0$ and $K = M$, we denote $\mathcal{S}$ as (M, M, N)-CCC.

Lemma 1 ([17])**.** *For an aperiodic $(K, M, N, \delta_{\max})$-QCSS, when $K \geq 3M, M \geq 2$ and $N \geq 2$, the parameters meet the inequality,*

$$\delta_{\max} \geq \sqrt{MN\left(1 - 2\sqrt{\frac{M}{3K}}\right)}. \tag{4}$$

To analyze the performance, the optimality factor ρ of QCSS is given in the following definition.

$$\rho = \frac{\delta_{\max}}{\sqrt{MN\left(1 - 2\sqrt{\frac{M}{3K}}\right)}}. \tag{5}$$

If $\rho = 1$, the aperiodic QCSS is optimal. The aperiodic QCSS is near-optimal when $1 < \rho \leq 2$.

3 Main Results

In this section, we first construct multiple asymptotically optimal aperiodic LC-CSSs with low inter-set cross-correlation property. By combining these LC-CSSs, a large-capacity aperiodic LC-CSS can be generated as a byproduct. Our proposed construction is then compared to the other construction method.

3.1 Multiple aperiodic LC-CSSs with low inter-set cross-correlation property

Prior to that, we introduce the subsequent Lemma. Note that the design of permutation $\pi_k^r(t)$ is inspired by [18].

Lemma 2. *$\pi_{k_1}^{r_1}(t) = r_1t^2 + t + k_1$, $\pi_{k_2}^{r_2}(t) = r_2t^2 + t + k_2$, where $1 \leq r_1, r_2 \leq p-1$, $0 \leq k_1, k_2 \leq p-1$. $\pi_{k_1}^{r_1}(t)$ and $\pi_{k_2}^{r_2}(t)$ are permutations of $\mathbb{Z}_p$ with following properties:*

1. *When $r_1 = r_2$ and $k_1 \neq k_2$, we have $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) \neq 0 \pmod p$, where $0 \leq t \leq p-1$;*
2. *When $r_1 \neq r_2$ and $k_1 = k_2$, there is only one solution t_1 with $t_1 = 0$ satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, where $0 \leq t \leq p-1$;*
3. *When $r_1 = r_2$ and $\tau \neq 0$, there is at most one solution t_1 with $0 \leq t_1 \leq p-1$ satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0 \pmod p$;*
4. *When $r_1 \neq r_2$, $k_1 = k_2$, $\tau \neq 0$ or $r_1 \neq r_2$, $k_1 \neq k_2$, there are at most two solutions t_1, t_2 with $0 \leq t_1, t_2 \leq p-1$ satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0 \pmod p$.*

Proof.
Case 1. When $1 \leq r_1 = r_2 \leq p-1$ and $0 \leq k_1 \neq k_2 \leq p-1$, $\pi_{k_1}^{r_1}(t)$ and $\pi_{k_2}^{r_2}(t)$ are both based on mapping from $\mathbb{Z}_p$ to $\mathbb{Z}_p$, thus $\pi_{k_1}^{r_1}(t) \neq \pi_{k_2}^{r_2}(t) \pmod p$. Therefore, the first property holds.
Case 2. When $1 \leq r_1 \neq r_2 \leq p-1$ and $0 \leq k_1 = k_2 \leq p-1$, suppose that $\pi_{k_1}^{r_1}(t) = \pi_{k_2}^{r_2}(t)$, then we have $r_1t^2 + t + k_1 = r_2t^2 + t + k_2$, calculate that $t_1 = 0 \pmod p$, it indicates that there is only one solution t_1 satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, where $0 \leq t \leq p-1$. Therefore, the second property holds.
Case 3. When $1 \leq r_1 = r_2 \leq p-1$, $0 \leq k_1, k_2 \leq p-1$ and $\tau \neq 0$, suppose that $\pi_{k_1}^{r_1}(t) = \pi_{k_2}^{r_2}(t+\tau)$, then we have $r_1t^2 + t + k_1 = r_2(t+\tau)^2 + (t+\tau) + k_2$, calculate that $t = \frac{k_1-k_2}{2r_2\tau} - \frac{r_2\tau+1}{2r_2} \pmod p$, it indicates that there is at most one solution t_1 satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0$, where $0 \leq t_1 \leq p-1$. Hence, the third property holds.
Case 4. When $1 \leq r_1 \neq r_2 \leq p-1$, $0 \leq k_1 = k_2 \leq p-1$, $\tau \neq 0$, or $1 \leq r_1 \neq r_2 \leq p-1$, suppose that $\pi_{k_1}^{r_1}(t) = \pi_{k_2}^{r_2}(t+\tau)$, we have $r_1t^2 + t + k_1 = r_2(t+\tau)^2 + (t+\tau) + k_2$, then we have $(r_1 - r_2)t^2 - (2r_2\tau)t - (k_2 - k_1 + r_2\tau^2 + \tau) = 0$, it indicates that there are at most two solutions t_1, t_2 satisfying $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, where $0 \leq t_1, t_2 \leq p-1$. Hence the forth property holds.

This completes the proof of Lemma 2.

□

The main construction is given as follows.

Construction 1. *Let $p \geq 3$ be a prime, $\mathbb{Z}_p$ denote the ring of integers modulo p, and $\omega_p = e^{2\pi\sqrt{-1}/p}$ be a primitive p-th root of unity. Let*

$$\pi_k^r(t) = rt^2 + t + k \pmod p. \tag{6}$$

Define a function $f_n^{(r,k,m)}: \mathbb{Z}_p \to \mathbb{Z}_p$ *as follows.*

$$f_n^{(r,k,m)}(t) = n \cdot \pi_k^r(t) + mt \pmod p, \tag{7}$$

where $1 \le r \le p-1$, $0 \le k, m, n, t \le p-1$. *Define* $p-1$ *sequence sets* $\mathcal{S}^r = \left\{\mathbf{S}^{(r,k,m)} : 0 \le k, m \le p-1\right\}$, *where*

$$\mathbf{S}^{(r,k,m)} = \begin{bmatrix} s_{0,0}^{(r,k,m)}, & s_{0,1}^{(r,k,m)}, & \cdots & s_{0,p-1}^{(r,k,m)} \\ s_{1,0}^{(r,k,m)}, & s_{1,1}^{(r,k,m)}, & \cdots & s_{1,p-1}^{(r,k,m)} \\ \vdots & \vdots & \ddots & \vdots \\ s_{p-1,0}^{(r,k,m)}, & s_{p-1,1}^{(r,k,m)}, & \cdots & s_{p-1,p-1}^{(r,k,m)} \end{bmatrix}, \tag{8}$$

and

$$s_{n,t}^{(r,k,m)} = \omega_p^{f_n^{(r,k,m)}(t)}. \tag{9}$$

Theorem 1. *Sequence sets* $\mathcal{S}^r$ *for* $1 \le r \le p-1$ *obtained from Construction 1 have following properties,*

1. *Each sequence set* $\mathcal{S}^r$ *is an aperiodic* (p^2, p, p, p)*-LC-CSS.*
2. *The inter-set cross-correlation between any two different LC-CSSs* $\mathcal{S}^{r_1}$ *and* $\mathcal{S}^{r_2}$ *is upper bounded by* $2p$, *i.e.,*

$$\left|\sum_{n=0}^{p-1} \widetilde{R}_{\mathbf{s}_n^{(r_1,k_1,m_1)}, \mathbf{s}_n^{(r_2,k_2,m_2)}}(\tau)\right| \le 2p, \tag{10}$$

for all $1 \le r_1 \ne r_2 \le p-1$, $0 \le \tau \le p-1$ *and* $0 \le k_1, k_2, m_1, m_2 \le p-1$.

Proof. First, let us prove Part 1.

Let $\mathbf{S}^{(r,k_1,m_1)}, \mathbf{S}^{(r,k_2,m_2)} \in \mathcal{S}^r$, where $1 \le r \le p-1$ and $0 \le k_1, k_2, m_1, m_2 \le p-1$. Then calculate the aperiodic correlation of $\mathbf{S}^{(r,k_1,m_1)}$ and $\mathbf{S}^{(r,k_2,m_2)}$ as following:

$$\begin{aligned} &\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)}, \mathbf{S}^{(r,k_2,m_2)}}(\tau) \\ &= \sum_{n=0}^{p-1} \widetilde{R}_{\mathbf{s}_n^{(r,k_1,m_1)}, \mathbf{s}_n^{(r,k_2,m_2)}}(\tau) \\ &= \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} s_{n,t}^{(r,k_1,m_1)} \cdot \left(s_{n,t+\tau}^{(r,k_2,m_2)}\right)^* \\ &= \omega_p^{-m_2\tau} \cdot \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} \omega_p^{t(m_1-m_2)+n\left(\pi_{k_1}^r(t) - \pi_{k_2}^r(t+\tau)\right)}. \end{aligned} \tag{11}$$

Consider the following four cases.

Case 1. When $k_1 = k_2$, $m_1 = m_2$ and $\tau = 0$, it is evident that $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)}, \mathbf{S}^{(r,k_2,m_2)}}(0) = p^2$.

Case 2. When $k_1 = k_2$, $m_1 \neq m_2$ and $\tau = 0$, then we have $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = p \cdot \sum_{t=0}^{p-1} \omega_p^{t(m_1-m_2)} = 0$.

Case 3. When $k_1 \neq k_2$ and $\tau = 0$, from the property 1 in Lemma 2, there is no solution t' for $\pi_{k_1}^r(t') - \pi_{k_2}^r(t') = 0 \pmod p$, thus $\sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t)-\pi_{k_2}^r(t+\tau)\right)} = 0$. Therefore, $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = 0$ holds.

Case 4. When $\tau \neq 0$, according to the property 3 in Lemma 2, there is at most one solution t' satisfying $\pi_{k_1}^r(t') - \pi_{k_2}^r(t'+\tau) = 0 \pmod p$.

If $t' \in [0, p-1-\tau]$, we have

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) \\
&= \omega_p^{-m_2\tau} \cdot \left[\omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t')-\pi_{k_2}^r(t'+\tau)\right)}\right. \\
&\quad \left. + \sum_{t=0,t\neq t'}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t)-\pi_{k_2}^r(t+\tau)\right)}\right] \\
&= p \cdot \omega_p^{t'(m_1-m_2)-m_2\tau}.
\end{aligned} \tag{12}$$

If $t' \in (p-1-\tau, p-1]$, then $\sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^r(t)-\pi_{k_2}^r(t+\tau)\right)} = 0$, thus $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = 0$. Otherwise, we have no solution t' satisfying $(\pi_{k_1}^r(t) - \pi_{k_2}^r(t+\tau) = 0 \pmod p)$, then $\widetilde{R}_{\mathbf{S}^{(r,k_1,m_1)},\mathbf{S}^{(r,k_2,m_2)}}(\tau) = 0$.

From the results of above four cases, we conclude that the maximum aperiodic correlation sidelobe amplitude value of $\mathcal{S}^r$ is $\delta_{\max} = p$.

Now we prove the Part 2.

Let $\mathbf{S}^{(r_1,k_1,m_1)} \in \mathcal{S}^{r_1}$, $\mathbf{S}^{(r_2,k_2,m_2)} \in \mathcal{S}^{r_2}$, where $1 \leq r_1 \neq r_2 \leq p-1$ and $0 \leq k_1, k_2, m_1, m_2 \leq p-1$. Similarly,

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&= \omega_p^{-m_2\tau} \cdot \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} \omega_p^{t(m_1-m_2)+n\left(\pi_{k_1}^{r_1}(t)-\pi_{k_2}^{r_2}(t+\tau)\right)}.
\end{aligned} \tag{13}$$

Consider the following two cases.

Case 1. When $r_1 \neq r_2, k_1 = k_2$ and $\tau = 0$, based on the property 2 in Lemma 2, there is only one solution t' with $t' = 0$ such that $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t) = 0 \pmod p$, then it holds

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&= \sum_{n=0}^{p-1} \sum_{t=0}^{p-1-\tau} \omega_p^{t(m_1-m_2)+n\left(\pi_{k_1}^{r_1}(t)-\pi_{k_2}^{r_2}(t)\right)} \\
&= \omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t')-\pi_{k_2}^{r_2}(t')\right)} + \sum_{t=0,t\neq t'}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t)-\pi_{k_2}^{r_2}(t)\right)} \\
&= p \cdot \omega_p^{t'(m_1-m_2)}.
\end{aligned} \tag{14}$$

Case 2. When $r_1 \neq r_2, k_1 = k_2, \tau \neq 0$, or $r_1 \neq r_2, k_1 \neq k_2$, according to the property 4 in Lemma 2, there are at most two solutions t' and t'' meeting $\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau) = 0$ (mod p).

Suppose that $t', t'' \in [0, p-1-\tau]$, we have

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&= \omega_p^{-m_2\tau} \cdot \left[\omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t') - \pi_{k_2}^{r_2}(t'+\tau)\right)} \right. \\
&\quad + \omega_p^{t''(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t'') - \pi_{k_2}^{r_2}(t''+\tau)\right)} \\
&\quad \left. + \sum_{t=0, t\neq t', t''}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau)\right)} \right] \\
&= p \cdot \omega_p^{-m_2\tau} \cdot \left(\omega_p^{t'(m_1-m_2)} + \omega_p^{t''(m_1-m_2)} \right).
\end{aligned} \tag{15}$$

Suppose that $t' \in [0, p-1-\tau]$, $t'' \in (p-1-\tau, p-1]$ or $t' \in [0, p-1-\tau]$, t'' unsolved, we have

$$\begin{aligned}
&\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \\
&= \omega_p^{-m_2\tau} \cdot \left[\omega_p^{t'(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t') - \pi_{k_2}^{r_2}(t'+\tau)\right)} \right. \\
&\quad \left. + \sum_{t=0, t\neq t'}^{p-1-\tau} \omega_p^{t(m_1-m_2)} \cdot \sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}(t+\tau)\right)} \right] \\
&= p \cdot \omega_p^{-m_2\tau + t'(m_1-m_2)}.
\end{aligned} \tag{16}$$

Suppose that $t', t'' \in (p-1-\tau, p-1]$, or $t' \in (p-1-\tau, p-1]$, t'' unsolved, then $\sum_{n=0}^{p-1} \omega_p^{n\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}('+\tau)\right)} = 0$, thus $\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) = 0$. Otherwise, we have no solution t' or t'' satisfying $\left(\pi_{k_1}^{r_1}(t) - \pi_{k_2}^{r_2}('+\tau)\right) = 0$ (mod p), hence $\widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) = 0$.

By summarizing the above discussion, we conclude that $\left| \sum_{n=0}^{p-1} \widetilde{R}_{\mathbf{S}^{(r_1,k_1,m_1)},\mathbf{S}^{(r_2,k_2,m_2)}}(\tau) \right| \leq 2p$ for $1 \leq r_1 \neq r_2 \leq p-1$, $0 \leq \tau \leq p-1$ and $0 \leq k_1, k_2, m_1, m_2 \leq p-1$.

Consequently, the proof of Theorem 1 is completed. □

Remark 1. According to Lemma 1, we get the limit of the optimality factor of $\mathcal{S}^r$ is

$$\lim_{p \to +\infty} \rho = \lim_{p \to +\infty} \frac{p}{\sqrt{p^2 \left(1 - 2\sqrt{\frac{p}{3p^2}}\right)}} = 1. \tag{17}$$

It implies that the aperiodic LC-CSS $\mathcal{S}^r$ generated from Construction 1 is asymptotically optimal.

3.2 Large-capacity aperiodic LC-CSS

We can use $p-1$ LC-CSSs with low inter-set aperiodic cross-correlation amplitude to generate a large-capacity aperiodic LC-CSS, as illustrated in the following.

Corollary 1. *Let $\mathcal{S} = \mathcal{S}^1 \cup \mathcal{S}^2 \cup \cdots \cup \mathcal{S}^{p-1}$, obtained $\mathcal{S}$ is a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS.*

Proof. Each sequence set $\mathcal{S}^r$ in Theorem 1 is a (p^2, p, p, p)-LC-CSS, where $1 \le r \le p-1$, and the intra-set maximum aperiodic cross-correlation amplitudes are p. According to Theorem 1, the inter-set aperiodic cross-correlation amplitudes are $2p$. Consequently, the set $\mathcal{S}$ is a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS. $\square$

Now calculate the optimality factor of $\mathcal{S}$. $\lim_{p\to+\infty} \rho = 2$. It indicates that aperiodic cross-correlation amplitudes of $\mathcal{S}$ asymptotically reaches twice concerning the correlation bound in Lemma 1.

In the following, we give an example to increase the readability of the construction in this paper.

Example 1. Let $p = 5$, we can generate four $(25, 5, 5, 5)$-LC-CSSs, $\mathcal{S}^1, \mathcal{S}^2, \mathcal{S}^3, \mathcal{S}^4$ from Theorem 1. The two LC-CSSs $\mathcal{S}^1$ and $\mathcal{S}^2$ are presented in Table **??**, where each element denotes a power of ω_5. The optimality factor of $\mathcal{S}^r (1 \le r \le 4)$ is $\rho = 1.4380$, which means that $\mathcal{S}^r$ is near-optimal. Moreover, we can combine these four LC-CSSs to obtain a large-capacity aperiodic $(100, 5, 5, 10)$-LC-CSS $\mathcal{S} = \mathcal{S}^1 \cup \mathcal{S}^2 \cup \mathcal{S}^3 \cup \mathcal{S}^4$ by Corollary 1. A brief overview of the correlation among the LC-CSSs is provided in Figure 1.

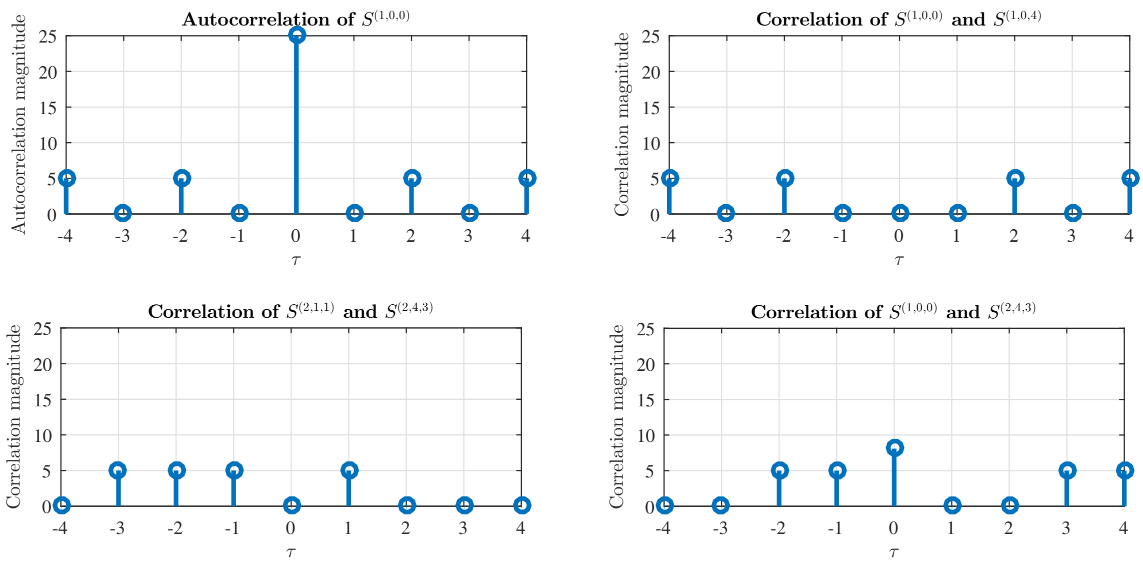

Figure 1: The correlation magnitudes of the LC-CSSs are illustrated in Example 1

Table 1: The two (25,5,5,5)-LC-CSSs $\mathcal{S}^1$ and $\mathcal{S}^2$ of Example 1

	$S^{(1,0,0)}$	$S^{(1,0,1)}$	$S^{(1,0,2)}$	$S^{(1,0,3)}$	$S^{(1,0,4)}$	$S^{(1,1,0)}$	$S^{(1,1,1)}$	$S^{(1,1,2)}$	$S^{(1,1,3)}$	$S^{(1,1,4)}$	$S^{(1,2,0)}$	$S^{(1,2,1)}$
	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321	00000	01234
	02120	03304	04033	00212	01441	13231	14410	10144	11323	12002	24342	20021
$\mathcal{S}^1$	04240	00424	01103	02332	03011	21412	22141	23320	24004	20233	43134	44313
	01310	02044	03223	04402	00131	34143	30322	31001	32230	33414	12421	13100
	03430	04114	00343	01022	02201	42324	43003	44232	40411	41140	31213	32442
$S^{(1,2,2)}$	$S^{(1,2,3)}$	$S^{(1,2,4)}$	$S^{(1,3,0)}$	$S^{(1,3,1)}$	$S^{(1,3,2)}$	$S^{(1,3,3)}$	$S^{(1,3,4)}$	$S^{(1,4,0)}$	$S^{(1,4,1)}$	$S^{(1,4,2)}$	$S^{(1,4,3)}$	$S^{(1,4,4)}$
02413	03142	04321	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321
21200	22434	23113	30403	31132	32311	33040	34224	41014	42243	43422	44101	40330
40042	41221	42400	10301	11030	12214	13443	14122	32023	33202	34431	30110	31344
14334	10013	11242	40204	41433	42112	43341	44020	23032	24211	20440	21124	22303
33121	34300	30034	20102	21331	22010	23244	24423	14041	10220	11404	12133	13312
	$S^{(2,0,0)}$	$S^{(2,0,1)}$	$S^{(2,0,2)}$	$S^{(2,0,3)}$	$S^{(2,0,4)}$	$S^{(2,1,0)}$	$S^{(2,1,1)}$	$S^{(2,1,2)}$	$S^{(2,1,3)}$	$S^{(2,1,4)}$	$S^{(2,2,0)}$	$S^{(2,2,1)}$
	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321	00000	01234
	03011	04240	00424	01103	02332	14122	10301	11030	12214	13443	20233	21412
$\mathcal{S}^2$	01022	02201	03430	04114	00343	23244	24423	20102	21331	22010	40411	41140
	04033	00212	01441	02120	03304	32311	33040	34224	30403	31132	10144	11323
	02044	03223	04402	00131	01310	41433	42112	43341	44020	40204	30322	31001
$S^{(2,2,2)}$	$S^{(2,2,3)}$	$S^{(2,2,4)}$	$S^{(2,3,0)}$	$S^{(2,3,1)}$	$S^{(2,3,2)}$	$S^{(2,3,3)}$	$S^{(2,3,4)}$	$S^{(2,4,0)}$	$S^{(2,4,1)}$	$S^{(2,4,2)}$	$S^{(2,4,3)}$	$S^{(2,4,4)}$
02413	03142	04321	00000	01234	02413	03142	04321	00000	01234	02413	03142	04321
22141	23320	24004	31344	32023	33202	34431	30110	42400	43134	44313	40042	41221
42324	43003	44232	12133	13312	14041	10220	11404	34300	30034	31213	32442	33121
12002	13231	14410	43422	44101	40330	41014	42243	21200	22434	23113	24342	20021
32230	33414	34143	24211	20440	21124	22303	23032	13100	14334	10013	11242	12421

3.3 Comparison with previous works

The most of existing parameters of aperiodic QCCSs are listed in Table 1. The QCSSs reported in [15, 10, 11] are constructed by combining multiple sets of CCCs, whereas our construction is based on combining multiple sets of LC-CSSs. When M and N is prime, this paper can obtain multiple subsets LC-CSSs and form a large set LC-CSS, which results in a larger set size than the literature [15, 9, 10, 11]. For example, when $M = N = 5$, one $(20, 5, 5, 5)$-LC-CSS can be provided from [15, 10, 11], one $(30, 5, 5, 5)$-LC-CSS can be generated from [9], four $(25, 5, 5, 5)$-LC-CSSs and one $(100, 5, 5, 10)$-LC-CSS can be obtained in this paper from Th.1 and Co.1.

Table 2: The parameters of aperiodic QCSSs

Ref.	Set size	Flock size	Sequence length	$\delta_{\max}$	Parameter condition(s)
Th.2 [15]	$p(p-1)$	p	p	p	$p \geq 3$ is a prime.
Th.1 [9]	$q(q+1)$	q	q	q	q is the power of a prime.
Th.3 [9]	q^2	q	$q-1$	q	$q \geq 5$ is the power of a prime.
Th.2 [10]	$N(p_0-1)$	N	N	N	$N \geq 5$ is an odd, and the minimum prime factor of N is p_0.
Th.4 [11]	$N \times F(N)$	N	N	N	$N \geq 2$ is an integer, $F(N)$ represents the largest number of rows that a Florentine rectangle of size $F(N) \times N$ can have.
Th.1 Proposed	p^2	p	p	p	$p \geq 3$ is a prime.
Co.1 Proposed	$p^2(p-1)$	p	p	$2p$	$p \geq 3$ is a prime.

4 Conclusion

This paper presents a method to construct multiple aperiodic LC-CSSs with low inter-set cross-correlation properties. Each aperiodic quasi-complementary sequence set is (p^2, p, p, p)-LC-CSS, and the parameters are asymptotically optimal. Moreover, a large-capacity aperiodic $(p^2(p-1), p, p, 2p)$-LC-CSS can be obtained by combining $p-1$ sequence sets. As communication technology improves, it is promising for researchers to create more various quasi-complementary sequences to meet communication system needs.

References

[1] A. Rathinakumar, A. K. Chaturvedi. Complete mutually orthogonal Golay complementary sets from Reed–Muller codes. *IEEE Trans. Inf. Theory*, 54(3):1339–1346, 2008.

[2] J. Tang, N. Zhang, Z. Ma, B. Tang. Construction of Doppler resilient complete complementary code in MIMO radar. *IEEE Trans. Signal Process.*, 62(18):4704–4712, 2014.

[3] S. Wang, A. Abdi. MIMO ISI channel estimation using uncorrelated Golay complementary sets of polyphase sequences. *IEEE Trans. Veh. Technol.*, 56(5):3024–3039, 2007.

[4] H. H. Chen, S. W. Chu, M. Guizani. On next generation CDMA technologies: The REAL approach for perfect orthogonal code generation. *IEEE Trans. Veh. Technol.*, 57(5):2822–2833, 2008.

[5] Z. Liu, U. Parampalli, Y. L. Guan, S. Boztas. Constructions of optimal and near-optimal quasi-complementary sequence sets from singer difference sets. *IEEE Wireless Commun. Lett.*, 2(5):487–490, 2013.

[6] A. Samad, S. Majhi. A near-optimal and low-complex joint multiuser detection for QCSS-MC-CDMA system. *IEEE Syst.*, 15(2):1594–1603, 2021.

[7] Y. Li, L. Tian, T. Liu, C. Xu. Constructions of quasi-complementary sequence sets associated with characters. *IEEE Trans. Inf. Theory*, 65(7):4597–4608, 2019.

[8] G. Luo, X. Cao, M. Shi, T. Helleseth. Three new constructions of asymptotically optimal periodic quasi-complementary sequence sets with small alphabet sizes. *IEEE Trans. Inf. Theory*, 67(8):5168–5177, 2021.

[9] Y. Li, L. Tian, C. Xu. Constructions of asymptotically optimal aperiodic quasi-complementary sequence sets. *IEEE Trans. Commun.*, 67(11):7499–7511, 2019.

[10] Z. Zhou, F. Liu, A. R. Adhikary, P. Fan. A generalized construction of multiple complete complementary codes and asymptotically optimal aperiodic quasi-complementary sequence sets. *IEEE Trans. Commun.*, 68(6):3564–3571, 2020.

[11] A. R. Adhikary, Y. Feng, Z. Zhou, P. Fan. Asymptotically optimal and near-optimal aperiodic quasi-complementary sequence sets based on Florentine rectangles. *IEEE Trans. Commun.*, 70(3):1475–1485, 2022.

[12] D. Li, C. Li, P. Sarkar. Asymptotically optimal quasi-complementary code sets of length $p_1^{m_1}p_2^{m_2}$. *Proc. 10th IEEE Int. Workshop Signal Des. Appl. Commun.*, 1–5, Colchester, United Kingdom, 2022.

[13] A. Roy, S. Majhi. Lower bounds on the maximum cross-correlations of 2-D quasi-complementary array sets. *Cryptogr. Commun.*, 1–19, 2023.

[14] Z. Zhou, D. Zhang, T. Helleseth, J. Wen. A construction of multiple optimal ZCZ sequence sets with good cross correlation. *IEEE Trans. Inf. Theory*, 64(2):1340–1346, 2018.

[15] T. Liu, C. Xu, Y. Li. Multiple complementary sequence sets with low inter-set cross-correlation property. *IEEE Signal Process. Lett.*, 26(6):913–917, 2019.

[16] P. Sarkar, C. Li, S. Majhi, Z. Liu. New correlation bound and construction of quasi-complementary sequence sets. *IEEE Trans. Inf. Theory*, 2024.

[17] Z. Liu, Y. L. Guan, W. H. Mow. A tighter correlation lower bound for quasi-complementary sequence sets. *IEEE Trans. Inf. Theory*, 60(1):388–396, 2014.

[18] P. Fan, M. H. Lee, D. Peng. New family of hopping sequences for time/frequency-hopping CDMA systems. *IEEE Wireless Commun. Lett.*, 4(6):2836–2842, 2005.