New Constructions of Mutually Orthogonal Complementary Sets and Z-Complementary Sequence Sets Based on Extended Boolean Functions

Hongyang Xiao
Nanjing University of Aeronautics and Astronautics
Xiwang Cao (xwcao@nuaa.edu.cn)
Nanjing University of Aeronautics and Astronautics

Research Article

Keywords: Multi-carrier code division multiple access (MC-CDMA), mutually orthogonal complementary sets (MOCSs), Z-complementary code sets (ZCCSs), extended Boolean functions (EBFs)

Posted Date: October 17th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2144533/v1

New Constructions of Mutually Orthogonal Complementary Sets and Z-Complementary Sequence Sets Based on Extended Boolean Functions

Hongyang Xiao*, Xiwang Cao†

Abstract

Mutually orthogonal complementary sets (MOCSs) have many applications in practical scenarios such as synthetic aperture imaging systems, orthogonal frequency division multiplexing code division multiple access (OFDM-CDMA) systems and multi-carrier code division multiple access (MC-CDMA) systems. Z-complementary code sets (ZCCSs) will be useful if the practical situation focuses more on the set size. Most of the known constructions of MOCSs and ZCCSs based on generalized Boolean functions (GBFs) have lengths with the form of 2^m or 2^m+2^t. Some constructions of MOCSs and ZCCSs based on other methods mostly have restrictive lengths. In this paper, we not only present constructions of an optimal ZCCS, but also construct MOCSs with flexible lengths. Both these constructions are based on extended Boolean functions. Though our proposed constructions generalize several previously known methods, we show that the parameters of these constructions are new and include previous parameters as special cases. In addition, a wide range of q-ary MOCSs and ZCCSs can be obtained by assigning different values to q.

Keywords: Multi-carrier code division multiple access (MC-CDMA)· mutually orthogonal complementary sets (MOCSs)· Z-complementary code sets (ZCCSs)· extended Boolean functions (EBFs).

Mathematics Subject Classification: 11T71 · 94A60 · 06E30

*Hongyang Xiao, College of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 211106, China, xhycxyf@163.com

†Corresponding author. Xiwang Cao, College of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 211106, China; Key Laboratory of Mathematical Modelling and High Performance Computing of Air Vehicles (NUAA), MIIT, Nanjing, 211106, China, xwcao@nuaa.edu.cn

1 Introduction

The term "complementary pair" was initiated by Golay in 1951 [1]. Golay complementary pair (GCP) is a pair of equal length sequences whose out-of-phase aperiodic auto-correlation sums are zeros. GCPs have extensive applications in wireless communication technology [2], radar [3], image processing [4], channel estimation [5], and peak power control in orthogonal frequency division multiplexing (OFDM) [6]. In 1972, Tseng and Liu generalized the concept of GCPs to Golay complementary sets (GCSs) and mutually orthogonal Golay complementary sets (MOCSs) [7]. A GCS which has the same aperiodic auto-correlation property as GCP is a set consisting of two or more sequences. Recently, many constructions of GCS have been proposed in [8–10]. An MOCS whose elements are mutually orthogonal in terms of their zero cross-correlation sums for all the time-shifts is a collection of GCSs, and it is also a set of M two-dimensional matrices of size $N \times L$, where M, N and L denote the set size, the flock size and the sequence length, respectively. In 1988, Suehiro and Hatori proposed the concept of complete complementary codes (CCCs) whose set size achieves the theoretical upper bound of MOCSs (i.e., $M \leq N$) [11]. MOCSs have been applied in many practical scenarios such as synthetic aperture imaging systems [4], OFDM-CDMA systems [12] and multi-carrier code division multiple access (MC-CDMA) systems [13–15]. Z-complementary code sets (ZCCSs) will be useful if the practical situation focuses more on the set size. In 2007, Fan *et al.* proposed the concept of Z-complementary code sets (ZCCSs) whose set size is much bigger than that of the CCCs system [16]. The reason why ZCCSs have large set size is that there is a zero correlation zone (ZCZ) in the aperodic cross-correlation and auto-correlation. For any (M, N, L, Z)-ZCCS, it holds that $M \leq N\lfloor L/Z \rfloor$ and it is optimal if the upper bound is achieved, where Z denotes the zero correlation zone (ZCZ) width. Especially, a set is called a mutually orthogonal complementary set (MOCS) if $Z = L$.

In recent years, the construction of complementary sequences based on generalized Boolean functions (GBFs) has attracted extensive attention in sequence design community. In order to meet the needs of more practical scenarios, some researchers take up researching optimal ZCCSs. However, most of these optimal ZCCSs based on GBFs have limited lengths [17–21]. To break this limitation, Shen *et al.* raised a new Boolean function and defined it as extended Boolean function (EBF) [22]. Unlike generalized Boolean functions, an extended Boolean function is a mapping from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$, where $\mathbb{Z}_q$ is the ring of integers modulo q and q is an arbitrary positive integer. Certainly, since the choice of q is arbitrary, there are some new practical applications in the sequence design community. Based on extended Boolean functions, Shen *et al.* proposed a $(q^{v+1}, q^v, q^m, q^{m-v})$-ZCCS. Inspired by their work, we not only propose an optimal ZCCS with certain lengths but also an MOCS with flexible lengths. In addition, the provided ZCCS has a bigger size than the ZCCS presented in [22].

The remainder of this paper is outlined as follows. In Section II, we give some definitions of complementary sequence sets and introduce extended Boolean functions. In Section III, we present a new MOCS and an optimal ZCCS with given lengths. Section IV shows a construction of MOCS with flexible lengths. Section V makes a comparison of the existing literature with this paper. Finally, Section VI concludes this paper.

2 Preliminaries

2.1 Notation

- $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ is the ring of integers modulo q, where q is an arbitrary positive integer throughout this paper, unless we specifically point out;
- $\mathbb{Z}_q^* = \mathbb{Z}_q \backslash \{0\}$;
- $\mathbb{N}_m = \{1, 2, \cdots, m\}$ is the set with m elements;
- $\xi = e^{2\pi\sqrt{-1}/q}$ is a primitive q-th root of unity;
- $\lfloor x \rfloor$ denotes the largest integer lower than or equal to x;
- Bold small letter $\mathbf{a}$ denotes a sequence of length L, i.e., $\mathbf{a} = (a_0, a_1, \cdots, a_{L-1})$;
- $(\cdot)^*$ denotes the conjugate of $(\cdot)$.

2.2 Correlation functions and complementary sequence sets

Assume $\mathbf{a} = (a_0, a_1, \cdots, a_{L-1})$ and $\mathbf{b} = (b_0, b_1, \cdots, b_{L-1})$ are $\mathbb{Z}_q$-valued sequences of length L, where a_i and b_i are in the ring $\mathbb{Z}_q$. The aperiodic cross-correlation function $R_{\mathbf{a},\mathbf{b}}(\tau)$ between $\mathbf{a}$ and $\mathbf{b}$ at a time shift τ is defined as

$$R_{\mathbf{a},\mathbf{b}}(\tau) = \begin{cases} \sum_{i=0}^{L-1-\tau} \xi^{a_i - b_{i+\tau}}, & 0 \le \tau \le L-1, \\ \sum_{i=0}^{L-1+\tau} \xi^{a_{i-\tau} - b_i}, & -L+1 \le \tau < 0. \end{cases}$$

If $\mathbf{a} = \mathbf{b}$, then $R_{\mathbf{a},\mathbf{b}}(\tau)$ is called the aperiodic autocorrelation function, denoted as $R_{\mathbf{a}}(\tau)$. In addition, by the definition of aperiodic correlation function, we get $R_{\mathbf{b},\mathbf{a}}(-\tau) = R^*_{\mathbf{a},\mathbf{b}}(\tau)$.

Definition 2.1. *A set of N length-L sequences $\{\mathbf{a}_0, \mathbf{a}_1, \cdots, \mathbf{a}_{N-1}\}$ is called a GCS of order N if for all $0 < |\tau| \le L-1$,*

$$\sum_{i=0}^{N-1} R_{\mathbf{a}_i}(\tau) = 0.$$

Definition 2.2. *A set of M sequence sets $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1, \cdots, \mathcal{S}_{M-1}\}$ is called an (M, N, L)-MOCS if for any i, j and τ with $0 \le i \ne j \le M-1$ and $0 \le |\tau| \le L-1$,*

$$R_{S_i,S_j}(\tau) = \sum_{k=0}^{N-1} R_{\mathbf{a}_{i,k},\mathbf{a}_{j,k}}(\tau) = 0,$$

where each $\mathcal{S}_t = \{\mathbf{a}_{t,0}, \mathbf{a}_{t,1}, \cdots, \mathbf{a}_{t,N-1}\}$ is a GCS of N length-L sequences.

Definition 2.3. *A set of M sequence sets $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1, \cdots, \mathcal{S}_{M-1}\}$ is called an (M, N, L, Z)-ZCCS if*

$$R_{S_i,S_j}(\tau) = \sum_{k=0}^{N-1} R_{\mathbf{a}_{i,k},\mathbf{a}_{j,k}}(\tau) = \begin{cases} NL, & \tau = 0,\ i = j, \\ 0, & 0 < |\tau| < Z,\ i = j, \\ 0, & |\tau| < Z,\ i \ne j, \end{cases}$$

where each $\mathcal{S}_t = \{\mathbf{a}_{t,0}, \mathbf{a}_{t,1}, \cdots, \mathbf{a}_{t,N-1}\}$ consists of N length-L sequences. In addition, if $Z = L$, then the (M, N, L, Z)-ZCCS is called an (M, N, L)-MOCS.

Lemma 2.4. *[11] For any (M, N, L)-MOCS, the upper bound of set size satisfies the inequality*

$$M \le N.$$

When $M = N$, it is also called a CCC.

Lemma 2.5. *[23] For any (M, N, L, Z)-ZCCS, it holds that*

$$M \le N \left\lfloor \frac{L}{Z} \right\rfloor.$$

A ZCCS is optimal if the above upper bound is achieved.

2.3 Extended Boolean functions (EBFs)

An extended Boolean function f in m variables $x_1, x_2, \cdots, x_m$ is a mapping from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$ where $x_i \in \mathbb{Z}_q$ for $i \in 1, 2, \cdots, m$. Given $f(x)$, we define

$$\mathbf{f} = (f_0, f_1, \cdots, f_{q^m-1}),$$

where $f_i = f(i_1, i_2, \cdots, i_m)$ and $(i_1, i_2, \cdots, i_m)$ is the q-ary representation of the integer $i = \sum_{k=1}^{m} i_k q^{k-1}$. For example, for $f = x_1x_2 + x_1 + 2$ with $m = 2$ and $q = 3$, we have the sequence $\mathbf{f} = (2, 0, 1, 2, 1, 0, 2, 2, 2)$. In addition, we also consider the sequences of length $L \ne q^m$. Hence we define the corresponding truncated sequence $f^{(L)}$ of the extended Boolean function f by removing the last $q^m - L$ elements of the sequence f. That is $f^{(L)} = (f_0, f_1, \cdots, f_{L-1})$ is a sequence of length L with $f_i = f(i_1, i_2, \cdots, i_m)$ for $i = 0, 1, \cdots, L-1$, which is a naturally generalization of [24]. For convenience, we ignore the superscript of $f^{(L)}$ unless the sequence length is undetermined.

3 Construction of optimal ZCCSs

In this section, we propose an approach to constructing an optimal ZCCS. Before doing this work, we need to construct a CCC as a preparing work.

Lemma 3.1. *[20] Suppose $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ for any $\alpha \in \{1, 2, \cdots, k\}$. Let us consider three conditions:*

(1) α_1 is the largest integer satisfying $i_{\pi_\alpha(\beta)} = j_{\pi_\alpha(\beta)}$ for $\alpha = 1, 2, \cdots, \alpha_1$ and $\beta = 1, 2, \cdots, m_\alpha$.

(2) β_1 is the smallest integer such that $i_{\pi_{\alpha_1}(\beta_1)} \neq j_{\pi_{\alpha_1}(\beta_1)}$.

(3) Let i' and j' be integers which differ from i and j, respectively, in only one position $\pi_{\alpha_1(\beta_1-1)}$, that is, $i'_{\pi_{\alpha_1(\beta_1-1)}} = 1 - i_{\pi_{\alpha_1(\beta_1-1)}}$ and $j'_{\pi_{\alpha_1(\beta_1-1)}} = 1 - j_{\pi_{\alpha_1(\beta_1-1)}}$.

If these above conditions are all satisfied, then we obtain $f_{n,i} - f_{n,j} - f_{n,i'} + f_{n,j'} \equiv \frac{q}{2} \ (mod\ q)$.

Theorem 3.2. *Let m, d be positive integers with $2 \leq d < m$, and $\{I_1, I_2, \cdots, I_d\}$ a partition of the set $\{1, 2, \cdots, m\}$. Put π_α be a bijection from $\{1, 2, \cdots, m_\alpha\}$ to I_α, where $|I_\alpha| = m_\alpha$ for any $\alpha \in \{1, 2, \cdots, d\}$. Let*

$$\begin{aligned} f(x) =& \sum_{\alpha=1}^{d} \sum_{\beta=1}^{m_\alpha-1} a_{\alpha,\beta} x_{\pi_\alpha(\beta)} x_{\pi_\alpha(\beta+1)} + \sum_{l=1}^{q-1} \sum_{u=1}^{m} h_{u,l} x_u^l + h_0, \\ f_n^p(x) =& f(x) + \sum_{\alpha=1}^{d} n_\alpha x_{\pi_\alpha(1)} + \sum_{\alpha=1}^{d} p_\alpha x_{\pi_\alpha(m_\alpha)}, \end{aligned}$$

where $a_{\alpha,\beta}, b \in \mathbb{Z}_q^*$ are co-prime with q, $h_{u,l}, h_0 \in \mathbb{Z}_q$, $(n_1, n_2, \cdots, n_d)$ and $(p_1, p_2, \cdots, p_d)$ are the q-ary representations of n and p, respectively. Then the set $\{F^0, F^1, \cdots, F^{q^d-1}\}$ forms a q-ary CCC with $F^p = \{f_0^p, f_1^p, \cdots, f_{q^d-1}^p\}$.

Proof. The proof consists of two parts. In the first part, we demonstrate that $\{F^p\}$ satisfies the ideal auto-correlation property, i.e., F^p is a GCS of size q^d for all $p \in \{0, 1, \cdots, q^d - 1\}$. We need to show that for any $0 < \tau \leq q^m - 1$ and $0 \leq p \leq q^d - 1$,

$$R(F^p; \tau) = \sum_{n=0}^{q^d-1} R(f_n^p; \tau) = \sum_{n=0}^{q^d-1} \sum_{i=0}^{q^m-1-\tau} \xi^{f_{n,i}^p - f_{n,i+\tau}^p} = \sum_{i=0}^{q^m-1-\tau} \sum_{n=0}^{q^d-1} \xi^{f_{n,i}^p - f_{n,i+\tau}^p} = 0,$$

where $f_{n,i}^p$ is the $(i+1)$-th element of sequence f_n^p. Throughout this paper, for a given integer i, we set $j = i + \tau$ and let $(i_1, i_2, \cdots, i_m)$ and $(j_1, j_2, \cdots, j_m)$ be the q-ary representations of i and j, respectively. Furthermore, we divide the set $\{i \mid 0 \leq i \leq q^m - 1 - \tau\}$ into two parts: $S_1(\tau) = \{i \mid \exists\ \alpha \in \{1, 2, \cdots, d\},\ 0 \leq i \leq q^m - 1 - \tau,\ i_{\pi_\alpha(1)} \neq j_{\pi_\alpha(1)}\}$ and

$S_2(\tau)=\{i \mid \forall\ \alpha\in\{1,2,\cdots,d\},\ 0\le i\le q^m-1-\tau,\ i_{\pi_\alpha(1)}=j_{\pi_\alpha(1)}\}$. Thus we obtain that

$$
\begin{aligned}
R(F^p;\tau) &= \sum_{i=0}^{q^m-1-\tau}\sum_{n=0}^{q^d-1}\xi^{f^p_{n,i}-f^p_{n,i+\tau}}\\
&= \sum_{i=0}^{q^m-1-\tau}\xi^{f_i-f_j}\prod_{\alpha=1}^{d}\left(\sum_{n_\alpha=0}^{q-1}\xi^{n_\alpha(i_{\pi_\alpha(1)}-j_{\pi_\alpha(1)})}\right)\\
&= \sum_{i\in S_1(\tau)}\xi^{f_i-f_j}\prod_{\alpha=1}^{d}\left(\sum_{n_\alpha=0}^{q-1}\xi^{n_\alpha(i_{\pi_\alpha(1)}-j_{\pi_\alpha(1)})}\right)\\
&\quad+\sum_{i\in S_2(\tau)}\xi^{f_i-f_j}\prod_{\alpha=1}^{d}\left(\sum_{n_\alpha=0}^{q-1}\xi^{n_\alpha(i_{\pi_\alpha(1)}-j_{\pi_\alpha(1)})}\right)\\
&=q^d\sum_{i\in S_2(\tau)}\xi^{f_i-f_j},
\end{aligned}
$$

where f_i is the $(i+1)$-th element of sequence f. For any $i\in S_2(\tau)$, we generalize the definition of Lemma 3.1:

(1) α_1 is the largest integer satisfying $i_{\pi_\alpha(\beta)}=j_{\pi_\alpha(\beta)}$ for $\alpha=1,2,\cdots,\alpha_1$ and $\beta=1,2,\cdots,m_\alpha$.

(2) β_1 is the smallest integer such that $i_{\pi_{\alpha_1}(\beta_1)}\neq j_{\pi_{\alpha_1}(\beta_1)}$.

(3) Let $i^{(t)}$ and $j^{(t)}$ be integers which differ from i and j, respectively, in only one position $\pi_{\alpha_1}(\beta_1-1)$, that is, $i^{(t)}_{\pi_{\alpha_1}(\beta_1-1)}=t\oplus i_{\pi_{\alpha_1}(\beta_1-1)}$ and $j^{(t)}_{\pi_{\alpha_1}(\beta_1-1)}=t\oplus j_{\pi_{\alpha_1}(\beta_1-1)}$.

Thus we get

$$f_{i^{(t)}}-f_i-f_{j^{(t)}}+f_j=ta_{\alpha_1,\beta_1-1}\left(i_{\pi_{\alpha_1}(\beta_1)}-j_{\pi_{\alpha_1}(\beta_1)}\right)$$

and

$$\xi^{f_i-f_j}+\xi^{f_{i^{(1)}}-f_{j^{(1)}}}+\xi^{f_{i^{(2)}}-f_{j^{(2)}}}+\cdots+\xi^{f_{i^{(q-1)}}-f_{j^{(q-1)}}}=0.$$

By the above two cases, we get that F^p is a GCS of size q^d.

In the second part, we demonstrate that for any $0\le p_1\neq p_2<q^d-1$, F^{p_1} and F^{p_2} satisfies the ideal corss-correlation property, i.e., for any $0<\tau<q^m$ and $0\le p_1\neq p_2\le q^d-1$,

$$R(F^{p_1},F^{p_2};\tau)=\sum_{n=0}^{q^d-1}R(f_n^{p_1},f_n^{p_2};\tau)=\sum_{n=0}^{q^d-1}\sum_{i=0}^{q^m-1-\tau}\xi^{f^{p_1}_{n,i}-f^{p_2}_{n,j}}=\sum_{i=0}^{q^m-1-\tau}\sum_{n=0}^{q^d-1}\xi^{f^{p_1}_{n,i}-f^{p_2}_{n,j}}=0,$$

where $f^{p_1}_{n,i}$ and $f^{p_2}_{n,j}$ are the $(i+1)$-th and the $(j+1)$-th element of sequence$f_n^{p_1}$ and $f_n^{p_2}$, respectively. In the same way, we divide the set $\{i\mid 0\le i\le q^m-1-\tau\}$ into two parts: $S_1(\tau)=\left\{i\mid \exists\ \alpha\in\{1,2,\cdots,d\},\ 0\le i\le q^m-1-\tau,\ i_{\pi_\alpha(1)}\ne j_{\pi_\alpha(1)}\right\}$ and $S_2(\tau)=\left\{i\mid \forall\ \alpha\in\{1,2,\cdots,d\},\ 0\le i\le q^m-1-\tau,\ i_{\pi_\alpha(1)}=j_{\pi_\alpha(1)}\right\}$. Thus we obtain that

$$\begin{aligned}
R(F^{p_1},F^{p_2};\tau)&=\sum_{i=0}^{q^m-1-\tau}\sum_{n=0}^{q^d-1}\xi^{f_{n,i}^{p_1}-f_{n,j}^{p_2}}\\
&=\sum_{i=0}^{q^m-1-\tau}\xi^{f_i-f_j}\prod_{\alpha=1}^{d}\left(\sum_{n_\alpha=0}^{q-1}\xi^{n_\alpha\left(i_{\pi_\alpha(1)}-j_{\pi_\alpha(1)}\right)}\right)\prod_{\alpha=1}^{d}\xi^{p_{1,\alpha}i_{\pi_\alpha(m_\alpha)}-p_{2,\alpha}j_{\pi_\alpha(m_\alpha)}}\\
&=\sum_{i\in S_1(\tau)}\xi^{f_i-f_j}\prod_{\alpha=1}^{d}\left(\sum_{n_\alpha=0}^{q-1}\xi^{n_\alpha\left(i_{\pi_\alpha(1)}-j_{\pi_\alpha(1)}\right)}\right)\prod_{\alpha=1}^{d}\xi^{p_{1,\alpha}i_{\pi_\alpha(m_\alpha)}-p_{2,\alpha}j_{\pi_\alpha(m_\alpha)}}\\
&+\sum_{i\in S_2(\tau)}\xi^{f_i-f_j}\prod_{\alpha=1}^{d}\left(\sum_{n_\alpha=0}^{q-1}\xi^{n_\alpha\left(i_{\pi_\alpha(1)}-j_{\pi_\alpha(1)}\right)}\right)\prod_{\alpha=1}^{d}\xi^{p_{1,\alpha}i_{\pi_\alpha(m_\alpha)}-p_{2,\alpha}j_{\pi_\alpha(m_\alpha)}}\\
&=q^d\sum_{i\in S_2(\tau)}\xi^{f_i-f_j}\prod_{\alpha=1}^{d}\xi^{p_{1,\alpha}i_{\pi_\alpha(m_\alpha)}-p_{2,\alpha}j_{\pi_\alpha(m_\alpha)}},
\end{aligned}$$

where $(p_{k,1},p_{k,2},\cdots,p_{k,d})$ is the q-ary representation of p_k for any $k\in\{1,2\}$. Likely, for any $i\in S_2(\tau)$, we use the generalization of Lemma 3.1 as above, then we have

$$f_{i^{(t)}}-f_i-f_{j^{(t)}}+f_j=ta_{\alpha_1,\beta_1-1}\left(i_{\pi_{\alpha_1}(\beta_1)}-j_{\pi_{\alpha_1}(\beta_1)}\right)$$

and

$$\xi^{f_i-f_j}+\xi^{f_{i^{(1)}}-f_{j^{(1)}}}+\xi^{f_{i^{(2)}}-f_{j^{(2)}}}+\cdots+\xi^{f_{i^{(q-1)}}-f_{j^{(q-1)}}}=0.$$

Combining these two cases, we know that the cross-correlation property is available for any $\tau>0$. Now, it remains to show that for any $0\le p_1\ne p_2\le q^d-1$ and $\tau=0$,

$$R(F^{p_1},F^{p_2};0)=\sum_{n=0}^{q^d-1}R(f_n^{p_1},f_n^{p_2};0)=\sum_{n=0}^{q^d-1}\sum_{i=0}^{q^m-1}\xi^{\sum_{\alpha=1}^{d}(p_{1,\alpha}\oplus p_{2,\alpha})i_{\pi_\alpha(m_\alpha)}}=0.$$

Put $\mathbf{d}=\sum_{\alpha=1}^{d}(p_{1,\alpha}\oplus p_{2,\alpha})\mathbf{x}_{\pi_\alpha(m_\alpha)}$. Due to that each sequence $\mathbf{x}_{\pi_\alpha(m_\alpha)}$ is a balaned sequence, the linear combination of these sequences of $\mathbf{x}_{\pi_1(m_1)},\mathbf{x}_{\pi_2(m_2)},\cdots,\mathbf{x}_{\pi_d(m_d)}$ is balanced, i.e., $\mathbf{d}$ is balanced. Then we have

$$R(f_n^{p_1},f_n^{p_2};0)=\sum_{n=0}^{q^d-1}\sum_{i=0}^{q^m-1}\xi^{\sum_{\alpha=1}^{d}(p_{1,\alpha}\oplus p_{2,\alpha})i_{\pi_\alpha(m_\alpha)}}=0,$$

which completes the proof.

□

With the help of the above theorem, the following $(q^{v+d},q^d,q^m,q^{m-v})$-ZCCS can be obtained easily.

Theorem 3.3. *Let m, d, v be positive integers with $d < m$ and $v < m$. Let $\{I_1, I_2, \cdots, I_d\}$ be a partition of the set $\{1, 2, \cdots, m - v\}$. Put π_α be a permutation from $\{1, 2, \cdots, m_\alpha\}$ to I_α, where $|I_\alpha| = m_\alpha$ for any $\alpha \in \{1, 2, \cdots, d\}$. Also let*

$$\begin{aligned} f(x) =& \sum_{\alpha=1}^{d} \sum_{\beta=1}^{m_\alpha-1} a_{\alpha,\beta} x_{\pi_\alpha(\beta)} x_{\pi_\alpha(\beta+1)} + \sum_{l=1}^{q-1} \sum_{u=1}^{m} h_{u,l} x_u^l + h_0, \\ f_n^p(x) =& f(x) + \sum_{\alpha=1}^{d} n_\alpha x_{\pi_\alpha(1)} + b \left(\sum_{\alpha=1}^{d} p_\alpha x_{\pi_\alpha(m_\alpha)} + \sum_{k=1}^{v} p_{k+d} x_{m-v+k} \right), \end{aligned}$$

where $(n_1, n_2, \cdots, n_d)$ and $(p_1, p_2, \cdots, p_{v+d})$ are the q-ary representations of n and p, respectively, $a_{\alpha,\beta}, b \in \mathbb{Z}_q^*$ are both co-prime with q, and $h_{u,l}, h_0 \in \mathbb{Z}_q$. Then $\{F^0, F^1, \cdots, F^{q^{v+d}-1}\}$ forms a $(q^{v+d}, q^d, q^m, q^{m-v})$-ZCCS with $F^p = \{f_0^p, f_1^p, \cdots, f_{q^d-1}^p\}$.

Proof. It is obvious that every sequence f_n^p can be divided into q^v relevant sub-sequence by a concatenate method, i.e.,

$$f_n^p = g_{n,0}^p | g_{n,1}^p | \cdots | g_{n,q^v-1}^p,$$

Each $g_{n,e}^p$ can be expressed as $g_{n,0}^p \oplus x$, i.e., $g_{n,e}^p = g_{n,0}^p \oplus x$, where $g_{n,e}^p$ denotes the $(e+1)$-th sub-sequence of f_n^p, $e \in \{0, 1, 2, \cdots, q^v - 1\}$ and $x \in \mathbb{Z}_q$. For any $0 < \tau \leq q^{m-v} - 1$ and any $0 < p \leq q^{v+d} - 1$,

$$\begin{aligned} R_{F^p}(\tau) &= \sum_{n=0}^{q^d-1} R_{f_n^p}(\tau) \\ &= \left(1 + \sum_{k=1}^{q^v-1} \xi^{u_k - w_k}\right) \sum_{n=0}^{q^d-1} R_{g_{n,0}^p}(\tau) + \left(\xi^{-w_1} + \sum_{k=1}^{q^v-2} \xi^{u_k - w_{k+1}}\right) \sum_{n=0}^{q^d-1} R^*_{g_{n,0}^p}(q^v - \tau) \\ &= 0. \end{aligned}$$

By the way of Theorem 3.2, we conclude that the sequence set $\{g_{0,0}^p, g_{1,0}^p, \cdots, g_{q^d-1,0}^p\}$ forms a GCS. Therefore, we know that $\{f_0^p, f_1^p, \cdots, f_{q^d-1}^p\}$ satisfies the auto-correlation property for $0 < \tau \leq q^{m-v} - 1$.

Next, we verify the cross-correlation property, i.e., for $0 \leq p_1 \neq p_2 \leq q^{v+d} - 1$ and for any $0 < \tau < q^{m-v}$,

$$\begin{aligned} & R_{F^{p_1}, F^{p_2}}(\tau) \\ =& \sum_{n=0}^{q^d-1} R_{f_n^{p_1}, f_n^{p_2}}(\tau) \\ =& \left(1 + \sum_{k=1}^{q^v-1} \xi^{u_k - w_k}\right) \sum_{n=0}^{q^d-1} R_{g_{n,0}^{p_1}, g_{n,0}^{p_2}}(\tau) + \left(\xi^{-w_1} + \sum_{k=1}^{q^v-2} \xi^{u_k - w_{k+1}}\right) \sum_{n=0}^{q^d-1} R^*_{g_{n,0}^{p_2}, g_{n,0}^{p_1}}(q^v - \tau) \\ =& 0, \end{aligned}$$

where $f_n^{p_1} = g_{n,0}^{p_1}|(g_{n,0}^{p_1} \oplus u_1)| \cdots |(g_{n,0}^{p_1} \oplus u_{q^v-1})$ and $f_n^{p_2} = g_{n,0}^{p_2}|(g_{n,0}^{p_2} \oplus w_1)| \cdots |(g_{n,0}^{p_2} \oplus w_{q^v-1})$ with $u_i, w_i \in \mathbb{Z}_q$. The q-ary representations of p_1 and p_2 are $(p_{1,1}, p_{1,2}, \cdots, p_{1,v+d})$ and $(p_{2,1}, p_{2,2}, \cdots, p_{2,v+d})$, respectively.

According to the definition of $f_n^p(x)$, we get that

$$g_{n,0}^p(x) = h(x) + \sum_{\alpha=1}^{d} n_\alpha x_{\pi_\alpha(1)} + b \sum_{\alpha=1}^{d} n_\alpha x_{\pi_\alpha(m_\alpha)},$$

where $h(x) = \sum_{\alpha=1}^{d} \sum_{\beta=1}^{m_\alpha-1} a_{\alpha,\beta} x_{\pi_\alpha(\beta)} x_{\pi_\alpha(\beta+1)} + \sum_{l=1}^{q-1} \sum_{u=1}^{m-v} h_{u,l} x_u^l + h_0$ with $\{I_1, I_2, \cdots, I_d\}$ a partition of the set $\{1, 2, \cdots, m-v\}$. Obviously, according to Theorem 3.2, we get that $\sum_{n=0}^{q^d-1} R_{g_{n,0}^{p_1}, g_{n,0}^{p_2}}(\tau) = 0$ and $\sum_{n=0}^{q^d-1} R^*_{g_{n,0}^{p_2}, g_{n,0}^{p_1}}(q^v - \tau) = 0$. This shows that $R_{F^{p_1}, F^{p_2}}(\tau) = 0$. Similarly, we can prove that $R_{F^{p_1}, F^{p_2}}(\tau) = 0$ for any $-q^d + 1 \leq \tau < 0$.

When $\tau = 0$, for any $0 \leq p_1 \neq p_2 \leq q^{v+d} - 1$,

$$R_{F^{p_1}, F^{p_2}}(0) = \sum_{n=0}^{q^d-1} \sum_{i=0}^{q^m-1} \prod_{\alpha=1}^{d} \xi^{b(p_{1,\alpha} \oplus p_{2,\alpha}) i_{\pi_\alpha(m_\alpha)}} \prod_{k=1}^{v} \xi^{b(p_{1,k+d} \oplus p_{2,k+d}) i_{m-v+k}} = 0.$$

The equality holds because $p_1 \neq p_2$ leads to the existence of at least one index $s \in \{1, 2, \cdots, v+d\}$ such that $p_{1,s} \neq p_{2,s}$ and $gcd(b, q) = 1$. By the above two cases, we get that $R_{f^{p_1}, f^{p_2}}(\tau) = 0$ for any $-q^d < \tau < q^d$ and $0 \leq p_1 \neq p_2 \leq q^{v+d}$. Thus we prove that $\{F^0, F^1, \cdots, F^{q^{v+d}-1}\}$ is a $(q^{v+d}, q^d, q^m, q^{m-v})$-ZCCS with $F^p = \{f_0^p, f_1^p, \cdots, f_{q^d-1}^p\}$.

$\square$

Remark 3.4. *According to Lemma 2.5, we know the ZCCS constructed from Theorem 3.3 is optimal since $M/N = q^{v+d}/q^d = L/Z$ is available. In particular, when $v = 0$, the Theorem 3.3 changes into Theorem 3.2.*

Example 3.5. *Let $a_{1,1} = b = 1$, $q = 4$, $m = 3$, $v = 1$, $d = 1$, $m_1 = 2$, $(\pi_1(1), \pi_1(2)) = (2, 1)$, $h_0 = 1$, $(h_{1,1}, h_{2,1}, h_{3,1}) = (1, 2, 2)$, $(h_{1,2}, h_{2,2}, h_{3,2}) = (3, 1, 0)$ and $(h_{1,3}, h_{2,3}, h_{3,3}) = (2, 1, 3)$ in Theorem 3.3. Then $\{F^0, F^1, \cdots, F^{15}\}$ forms a quaternary $(16, 4, 64, 16)$-ZCCS, where F^3 and F^{10} are given by*

$$\begin{bmatrix} f_0^3 \\ f_1^3 \\ f_2^3 \\ f_3^3 \end{bmatrix} = \begin{bmatrix} 1212133132323311121213313232331112121331323233111212133132323311 \\ 1212200210102200121220021010220012122002101022001212200210102200 \\ 1212311332321133121231133232113312123113323211331212311332321133 \\ 1212022010100022121202201010002212120220101000221212022010100022 \end{bmatrix}$$

$$\begin{bmatrix} f_0^{10} \\ f_1^{10} \\ f_2^{10} \\ f_3^{10} \end{bmatrix} = \begin{bmatrix} 1133121231133232331130301331101011331212311332323311303013311010 \\ 1133232313312121331101013111303031133232313312121331101013111303 \\ 1133303031131010331112121331323211333030311310103311121213313232 \\ 1133010113310303331123233113212111330101133103033311232331132121 \end{bmatrix}$$

The sum of aperiodic auto-correlation of sequences F^3 is presented in Figure 1 and the sum of aperiodic cross-correlation of sequences F^3 and F^{10} is presented in Figure 2.

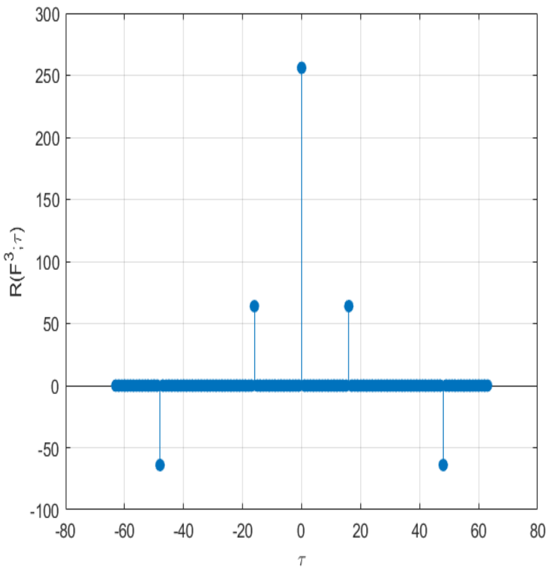

Figure 1: the sum of aperiodic auto-correlation of sequences F^3

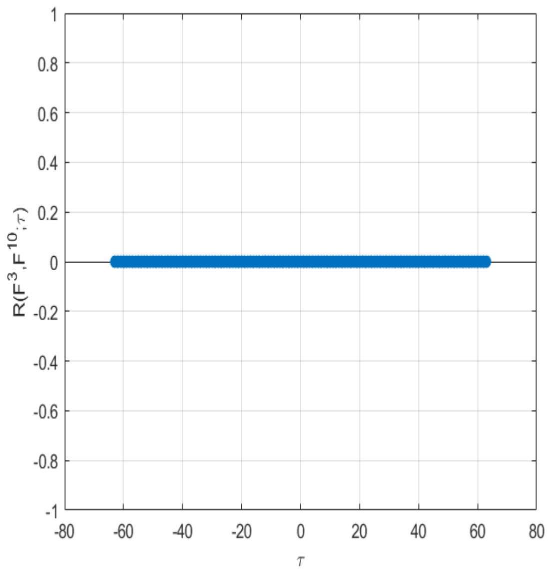

Figure 2: the sum of aperiodic cross-correlation of sequences F^3 and F^{10}

4 Construction of MOCSs with flexible lengths

In this section, we present a direct construction of MOCSs with flexible lengths. Before giving the construction of MOCSs, we introduce the following lemma.

Lemma 4.1. *[8] For an even integer q and any positive integers m, k with $k \leq m$, let v be an integer with $0 \leq v \leq m-k$, and π be a permutation of $\{1, 2, \cdots, m\}$ satisfying the following three conditions:*

(1) $\pi(m-k+1) < \pi(m-k+2) < \cdots < \pi(m-1) < \pi(m) = m$.

(2) *If $v > 0$, then $\{\pi(1), \pi(2), \cdots, \pi(v)\} = \{1, 2, \cdots, v\}$.*

(3) *For all $\alpha = 1, 2, \cdots, k-1$, if $\pi(t) < \pi(m-k+\alpha)$, then $\pi(t-1) < \pi(m-k+\alpha)$ where $2 \leq t \leq m-k$.*

For the generalized Boolean function

$$f = \frac{q}{2}\sum_{s=1}^{m-k-1} x_{\pi(s)}x_{\pi(s+1)} + \sum_{\alpha}^{k}\sum_{s=1}^{m-k} c_{\alpha,s}x_{\pi(m-k+\alpha)}x_{\pi(s)} + \sum_{s=1}^{m} c_s x_s + c_0,$$

where $c_{\alpha,s}, c_s \in \mathbb{Z}_q$, the set

$$F = \left\{ f + \frac{q}{2}\sum_{\alpha=1}^{k} d_\alpha x_{\pi(m-k+\alpha)} + \frac{q}{2} d_{k+1} x_{\pi(1)} \mid d_\alpha \in \{0,1\} \right\}$$

is a GCS of size 2^{k+1} and length $L = 2^{m-1} + \sum_{\alpha=1}^{k-1} a_\alpha 2^{\pi(m-k+\alpha)-1} + 2^v$ where $a_\alpha \in \{0,1\}$.

Lemma 4.2. *For positive integers $m \geq 2$ and $N < m$, let h be a bijection function from $S_1 = \{1, 2, \cdots, N\}$ onto a subset of $\{1, 2, \cdots, m\}$ with N elements. Then there exists a smallest element $h(u)$ for $u \in S_1$. Let i be an integer with*

$$\sum_{\substack{l=1\\ l\neq u}}^{N} c_l q^{h(l)-1} \leq i \leq \sum_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1} + q^{h(u)} - 1,$$

where $a_l \in \mathbb{Z}_q$ for $l \in S_1 \setminus \{u\}$ and $(i_1, i_2, \cdots, i_m)$ is the q-ary representation of i. Also let $i^{(t)}$ be an integer with q-ary representation $(i_1, i_2, \cdots, i_k \oplus t, \cdots, i_m)$ for positive integers $k \leq h(u)$ and $t \in \mathbb{Z}_q^*$. Then we have

$$\sum_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1} \leq i^{(t)} \leq \sum_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1} + q^{h(u)} - 1.$$

Proof. For convenience, we let $j = i - \sum\limits_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1}$ and $(j_1, j_2, \cdots, j_m)$ be the q-ary representation of j. Then $0 \leq j \leq q^{h(u)} - 1$, which means $j_s = 0$ for $s \geq h(u) + 1$. Similarly, we let $j^{(t)} = i^{(t)} - \sum\limits_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1}$ with q-ary representation $(j_1, j_2, \cdots, j_k \oplus t, \cdots, j_m)$. Obviously, the q-ary representation of j differs from that of $j^{(e)}$ in only one position t. So we obtain $j_s^{(t)} = j_s = 0$ for $s \geq h(u) + 1$ which implies $0 \leq j^{(t)} \leq q^{h(u)} - 1$. Therefore,

$$\sum_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1} \leq i^{(t)} \leq \sum_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1} + q^{h(u)} - 1.$$

□

Lemma 4.3. *For positive integers $m \geq 2$ and $N < m$, let i and function h be the same as that of lemma 4.2. If $i \leq \sum\limits_{\substack{l=1\\ l\neq u}}^{N} a_l q^{h(l)-1} + q^{h(u)} - 1$ and $i_{h(l)} = a_l$ for $l \in S_1 \setminus \{u\}$. Then we have $i_s = 0$ for $s = h(u)+1, h(u)+2, \cdots, m-1$ and $s \neq h(l)$ for $l \in S_1 \setminus \{u\}$.*

Proof. Suppose the conclusion doesn't hold, we assume $i_t = 1$ where $h(u)+1 \le t \le m-1$ and $t \ne h(l)$ for $l \in S_1 \setminus \{u\}$. Then we have $i \ge \sum_{\substack{l=1\\ l\ne u}}^{N} a_l q^{h(l)-1} + q^t \ge \sum_{\substack{l=1\\ l\ne u}}^{N} a_l q^{h(l)-1} + q^{h(u)}$ which contradicts the condition. □

Lemma 4.4. *Let $\boldsymbol{x}_{n_1}, \boldsymbol{x}_{n_2}, \cdots, \boldsymbol{x}_{n_d}$ be the suquences corresponding to extended Boolean functions $x_{n_1}, x_{n_2}, \cdots, x_{n_d}$, respectively, where $n_1 < n_2 < \cdots < n_d$. Let a q-ary sequence $\boldsymbol{d}_2 = a_1\boldsymbol{x}_{n_1} \oplus a_2\boldsymbol{x}_{n_2} \oplus \cdots \oplus a_d\boldsymbol{x}_{n_d}$ be the linear combination of $\boldsymbol{x}_{n_1}, \boldsymbol{x}_{n_2}, \cdots, \boldsymbol{x}_{n_d}$ with $a_i \in Z_q$ for any $i \in \{1, 2, \cdots, d\}$. If $q^{n_1} \mid L$, we assume that the sequence $\boldsymbol{d}_2$ is balanced and the Hamming weight of $\boldsymbol{d}_2$ is $\frac{L}{q}$.*

Now we state our construction in the following theorem, which is based on Lemma 4.1.

Theorem 4.5. *Let m, d, v be positive integers with $2 \le d < m$ and $v < m$. Let I_1, I_2, $\cdots$, I_d be a partition of the set $\{1, 2, \cdots, m-v\}$. Put π_α be a bijiection from $\{1, 2, \cdots, m_\alpha\}$ to I_α, where $|I_\alpha| = m_\alpha$ for any $\alpha \in \{1, 2, \cdots, d\}$. Let u be an integer with $0 \le u \le m_1$, if $u > 0$, we impose an additional condition below:*

$$\{\pi_1(1), \pi_1(2), \cdots, \pi_1(u)\} = \{1, 2. \cdots, u\}.$$

Let $(n_1, n_2, \cdots, n_{d+v})$ and $(p_1, p_2, \cdots, p_d)$ be the q-ary representations of n and p, respectively. Let

$$f(x) = \sum_{\alpha=1}^{d}\sum_{\beta=1}^{m_\alpha-1} a_{\alpha,\beta} x_{\pi_\alpha(\beta)} x_{\pi_\alpha(\beta+1)} + \sum_{\alpha=1}^{d}\sum_{\beta=1}^{m_\alpha}\sum_{k=1}^{v} b_{\alpha,\beta,k} x_{\pi_\alpha(\beta)} x_{m-v+k} + \sum_{s=1}^{m} c_{s,l} x_s^l + c_0,$$

$$f_n^p(x) = f(x) + \sum_{\alpha=1}^{d} n_\alpha x_{\pi_\alpha(1)} + \sum_{k=1}^{v} n_{k+d} x_{m-v+k} + c\sum_{\alpha=1}^{d} p_\alpha x_{\pi_\alpha(m_\alpha)},$$

where $a_{\alpha,\beta}, c \in \mathbb{Z}_q^*$ are co-prime with q and $b_{\alpha,\beta,k}, c_s \in \mathbb{Z}_q$. Then $\{F^0, F^1, \cdots, F^{q^d-1}\}$ generates a (q^d, q^{v+d}, L)-MOCS with $L = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u$ and $a_m \in \mathbb{Z}_q^*$, where $F^p = \{f_0^p, f_1^p, \cdots, f_{q^{v+d}-1}^p\}$

Proof. The proof can also be divided into two parts. In the first part, we demonstrate that F^p is a GCS for any $p \in \mathbb{Z}_{q^d}$. Since $R_{f_n^p}(-\tau) = R^*_{f_n^p}(\tau)$ for any sequence f_n^p, it suffices to show that for any $0 < \tau \le L-1$,

$$R_{F^p}(\tau) = \sum_{n=0}^{q^{v+d}-1}\sum_{i=0}^{L-1-\tau} \xi^{f_{n,i}^p - f_{n,i+\tau}^p} = \sum_{i=0}^{L-1-\tau}\sum_{n=0}^{q^{v+d}-1} \xi^{f_{n,i}^p - f_{n,i+\tau}^p} = 0.$$

Similarly, let the definitions of $i, j, i^{(t)}$ and $j^{(t)}$ be given as Theorem 3.2.

Case 1: If $i_{\pi_\alpha(1)} \neq j_{\pi_\alpha(1)}$ for some $\alpha \in \{1,2,\cdots,d\}$ or $i_{m-v+k} \neq j_{m-v+k}$ for some $k \in \{1,2,\cdots,v\}$. Then

$$R(F^p;\tau) = \sum_{i=0}^{L-1-\tau} \xi^{f_i - f_j} \prod_{\alpha=1}^{d} \left(\sum_{n_\alpha=0}^{q-1} \xi^{n_\alpha \left(i_{\pi_\alpha(1)} - j_{\pi_\alpha(1)}\right)} \right) \prod_{\alpha=1}^{d} \xi^{p_\alpha \left(i_{\pi_\alpha(m_\alpha)} - j_{\pi_\alpha(m_\alpha)}\right)} A = 0.$$

where $A = \prod_{k=1}^{v} \left(\sum_{n_{d+k}=0}^{q-1} \xi^{n_{d+k}(i_{m-v+k} - j_{m-v+k})} \right) = 0$.

Case 2: If $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ for all $\alpha \in \{1,2,\cdots,d\}$, $i_{m-v+k} = j_{m-v+k}$ for all $k \in \{1,2,\cdots,v\}$, and $i_m = j_m = 0$. Then according to generalization of Lemma 4.3, we can get

$$\xi^{f_i - f_j} + \sum_{t=1}^{q-1} \xi^{f_{i^{(t)}} - f_{j^{(t)}}} = \xi^{f_i - f_j} \left(1 + \sum_{t=1}^{q-1} \xi^{a_{\alpha_1,\beta_1-1} t \left(i_{\pi_{\alpha_1}(\beta_1)} - j_{\pi_{\alpha_1}(\beta_1)}\right)} \right) = 0,$$

which implies

$$R_{F^p}(\tau) = \sum_{n=0}^{q^{v+d}-1} \sum_{i=0}^{L-1-\tau} \xi^{f^p_{n,i} - f^p_{n,j}} = 0.$$

Case 3: $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ for all $\alpha \in \{1,2,\cdots,d\}$, $i_{m-v+k} = j_{m-v+k}$ for all $k \in \{1,2,\cdots,v\}$, and $i_m = j_m = a_m \neq 0$. Suppose k_1 is the largest integer such that $i_{m-v+k} = j_{m-v+k} = 0$ for $k_1 < v$, i.e., $i_{m-v+k} = j_{m-v+k} = a_k$ for $k \in \{k_1+1, k_1+2, \cdots, v\}$, then

$$\begin{aligned} i,j < L &= a_m q^{m-1} + \sum_{\alpha=1}^{v-1} a_k q^{m-v+k-1} + q^u \\ &\leq a_m q^{m-1} + \sum_{k=k_1+1}^{v-1} a_k q^{m-v+k-1} + q^{m-v+k_1-1} - 1. \end{aligned}$$

According to Lemma 4.2 and $\pi_{\alpha_1(\beta_1-1)} < q^{m-v+k_1-1}$, we have

$$i^{(t)}, j^{(t)} \leq a_m q^{m-1} + \sum_{k=k_1+1}^{v-1} a_k q^{m-v+k-1} + q^{m-v+k_1-1} - 1 < L.$$

Therefore, we get

$$\xi^{f_i - f_j} + \xi^{f_{i^{(1)}} - f_{j^{(1)}}} + \cdots + \xi^{f_{i^{(q-1)}} - f_{j^{(q-1)}}} = 0.$$

Case 4: $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ for all $\alpha \in \{1,2,\cdots,d\}$, $i_{m-v+k} = j_{m-v+k}$ for all $k \in \{1,2,\cdots,v\}$, and $i_m = j_m = a_m \neq 0$. We also consider that $i_{m-v+k} = j_{m-v+k} = a_k \neq 0$ for all $k \in \{1,2,\cdots,v\}$,

$$i,j < L = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u.$$

According to Lemma 4.3, we have $i_s = j_s = 0$ for $s = u+1, u+2, \cdots, m-v-1$, so $\pi_{\alpha_1}(\beta_1) \leq u$. Note that we do not need to consider $u = 0$ in this case. If we assume $u = 0$, then we have $j = i$, which means $\tau = 0$. Therefore,

$$i^{(t)}, j^{(t)} \leq a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u < L$$

and

$$\xi^{f_i - f_j} + \xi^{f_{i^{(1)}} - f_{j^{(1)}}} + \cdots + \xi^{f_{i^{(q-1)}} - f_{j^{(q-1)}}} = 0.$$

Combining the above four cases, we can conclude that F^p is a GCS of length $L = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u$.

In the second part, we prove that F^{p_1} and F^{p_2} satisfy the ideal cross-correlation property for any different $0 \leq p_1 \neq p_2 \leq q^d - 1$, i.e., for any $0 < \tau \leq L-1$,

$$R_{F^{p_1}, F^{p_2}}(\tau) = \sum_{i=0}^{L-1-\tau} \sum_{n=0}^{q^{v+d}-1} \xi^{f_{n,i}^{p_1} - f_{n,j}^{p_2}} = 0.$$

In the same way, let the definitions of $i, j, i^{(t)}, j^{(t)}, u$ be given as Theorem 3.2.

Case 1: If $i_{\pi_\alpha(1)} \neq j_{\pi_\alpha(1)}$ for some $\alpha \in \{1, 2, \cdots, d\}$ or $i_{m-v+k} \neq j_{m-v+k}$ for some $k \in \{1, 2, \cdots, v\}$. Then

$$R_{F^{p_1}, F^{p_2}}(\tau) = \sum_{i=0}^{L-1-\tau} \xi^{f_i - f_j} \prod_{\alpha=1}^{d} \xi^{\left(p_{1,\alpha} i_{\pi_\alpha(m_\alpha)} - p_{2,\alpha} j_{\pi_\alpha(m_\alpha)}\right)} B = 0,$$

where $B = \prod_{\alpha=1}^{d} \left(\sum_{n_\alpha=0}^{q-1} \xi^{n_\alpha \left(i_{\pi_\alpha(1)} - j_{\pi_\alpha(1)}\right)} \right) \prod_{k=1}^{v} \left(\sum_{n_{d+k}=0}^{q-1} \xi^{n_{d+k}(i_{m-v+k} - j_{m-v+k})} \right) = 0.$

Case 2: If $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ for all $\alpha \in \{1, 2, \cdots, d\}$, $i_{m-v+k} = j_{m-v+k}$ for all $k \in \{1, 2, \cdots, v\}$, and $i_m = j_m$. Then according to generalization of Lemma 4.3, we can get

$$\xi^{f_i - f_j} + \sum_{t=1}^{q-1} \xi^{f_{i^{(t)}} - f_{j^{(t)}}} = \xi^{f_i - f_j} \left(1 + \sum_{t=1}^{q-1} \xi^{a_{\alpha_1, \beta_1 - 1} t \left(i_{\pi_{\alpha_1}(\beta_1)} - j_{\pi_{\alpha_1}(\beta_1)} \right)} \right) = 0,$$

which implies

$$R_{F^{p_1}, F^{p_2}}(\tau) = \sum_{n=0}^{q^{v+d}-1} \sum_{i=0}^{L-1-\tau} \xi^{f_{n,i}^{p_1} - f_{n,j}^{p_2}} = \sum_{i=0}^{L-1-\tau} \sum_{n=0}^{q^{v+d}-1} \xi^{f_{n,i}^{p_1} - f_{n,j}^{p_2}} = 0.$$

From Case 1 and Case 2, we can obtain that $R_{F^{p_1}, F^{p_2}}(\tau) = 0$ holds for $\tau > 0$. Now, it remains to show that

$$R_{F^{p_1}, F^{p_2}}(0) = \sum_{n=0}^{q^{v+d}-1} \sum_{i=0}^{L-1} \xi^{f_{n,i}^{p_1} - f_{n,i}^{p_2}} = 0.$$

Table 1: Summary of Existing MOCSs

Source	Based on	Parameters	Conditions
[25]	GBF	$(2^{k'}, 2^{k+1}, 2^m + 2^t)$	$0 < k, t \leq m; 0 \leq k' \leq t; k' \leq k-1$
[25]	GBF	$(2^k, 2^{k+1}, 2^m + 2^t)$	$0 < k \leq t \leq m$
[26]	GBF	$(2^k, 2^k, 2^m)$	$0 < k \leq m$
[32]	GBF	$(2^k, 2^k, 2^m)$	$k, m > 0$
[33]	GBF	$(2^k, 2^{k+1}, 2^m + 2^t)$	$0 \leq t < k \leq m$
[34]	PU matrix	(M, M, M^m)	$m > 0$
[35]	PU matrix	(M, M, N^m)	$N \mid M, m > 0$
[36]	(M, L_2)-CCC	(M, MN, L_1L_2)	M is even
[37]	multivariable function	$(\prod_{i=1}^k p_i, \prod_{i=1}^k p_i, \prod_{i=1}^k p_i^{m_i})$	$p_\alpha \mid q$, q is a finite positive integer, $\alpha = 1, 2, \cdots, k$
[38]	GBF	$(2^{k+1}, 2^{k+1}, 2^{m-1} + 2^{m-3})$	$k \leq m-5$
[39]	PU matrix	(M, M, M^N)	$N \geq 1$
[40]	Kronecker product	(M_1M_2, M_1M_2, N_1N_2)	$(M_1, M_1, N_1) - CCC$, and $(M_2, M_2, N_2) - CCC$ exists
[41]	Kronecker product	(M, M, MN_1N_2)	$(M, M, N_1) - CCC$, and $(M, M, N_2) - CCC$ exists
Theorem 3.2	EBF	(q^d, q^d, q^m)	$0 < d < m$, q is an arbitrary positive integer
Theorem 4.5	EBF	(q^d, q^{v+d}, L)	$0 < d < m$, q is an arbitrary positive integer

For any nonnegative integer $n < q^{v+d}$, we have

$$f_{n,i}^{p_1} - f_{n,i}^{p_2} = c\left(\sum_{\alpha=0}^{d}(p_{1,\alpha} - p_{2,\alpha})i_{\pi_\alpha(m_\alpha)}\right),$$

where $(p_{1,1},, p_{1,2}, \cdots, p_{1,k})$ and $(p_{2,1},, p_{2,2}, \cdots, p_{2,k})$ are the q-ary representations of p_1 and p_2, respectively. Since the sequence of $(p_{1,\beta} - p_{2,\beta})i_{\pi(m-k+\beta)}$ is balanced according to Lemma 4.4, then we have $\xi^{f_{n,i}^{p_1} - f_{n,i}^{p_2}} + \xi^{f_{n,i(1)}^{p_1} - f_{n,i(1)}^{p_2}} + \xi^{f_{n,i(q-1)}^{p_1} - f_{n,i(q-1)}^{p_2}} = 0$. Therefore, we get

$$R_{F^{p_1}, F^{p_2}}(0) = \sum_{n=0}^{q^{k+1}-1}\sum_{i=0}^{L-1}\xi^{f_{n,i}^{p_1} - f_{n,i}^{p_2}} = 0.$$

By the above discussion, we obtain that $\{F^p \mid p \in \mathbb{Z}_{q^d}\}$ is a (q^d, q^{v+d}, L)-MOCS.

$\square$

Remark 4.6. *In Theorem 4.5, if we let $q = 2$ and all $a_k = 0$ and $a_m = 1$, then the length $L = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u$ turns into the form $2^{m-1} + 2^u$, this result is covered in [25].*

Example 4.7. *Let $a_{1,1} = c = 1$, $q = 4$, $m = 3$, $v = 1$, $d = 1$, $m_1 = 2$, $(\pi_1(1), \pi_1(2)) = (1, 2)$, $h_0 = 1$, $(b_{1,1,1}, b_{1,2,1}) = (3, 2)$, $c_s = 0$, $a_3 = 3$ and $u = 1$ in Theorem 4.5. Then $\{F^0, F^1, \cdots, F^3\}$ forms a quaternary $(4, 16, 52)$-MOCS.*

5 Comparison

Table 1 and Table 2 show the existence of constructions of MOCSs and ZCCSs in previous papers. The notation "$\surd$" (resp. "$\times$") in Table 2 means the corresponding ZCCSs are optimal (resp. non-optimal).

Table 2: Summary of Existing ZCCSs

Source	Based on	Parameters	Conditions	Optimal	Remark
[17]	GBF	$(2^n, 2^n, 2^{m-1}+2, 2^{m-2}+2^{\pi(m-3)}+1)$	$m \geq 3$	$\surd$	Direct
[18]	GBF	$(2^{n+p}, 2^n, 2^m, 2^{m-p})$	$p \leq m$	$\surd$	Direct
[19]	GBF	$(2^{k+p+1}, 2^{k+1}, 2^m, 2^{m-p})$	$k+p \leq m$	$\surd$	Direct
[20]	GBF	$(2^{k+v}, 2^k, 2^m, 2^{m-v})$	$v \leq m, k \leq m-v$	$\surd$	Direct
[21]	GBF	$(2^{k+1}, 2^{k+1}, 3\cdot 2^m, 2^{m+1})$	$k \leq m$	$\times$	Direct
[22]	EBF	$(q^{v+1}, q, q^m, q^{m-v})$	$v \leq m$	$\surd$	Direct
[21]	GBF	$(2^{k+2}, 2^{k+2}, 2^m \cdot L, 2^m \cdot L')$	$L' > \frac{L}{2}$	$\surd$	Direct
[27]	Butson-type Hadamard Matrices	(MP, M, MP, M)	$M \geq 2, P > 0$	$\surd$	Indirect
[27]	Optimal ZPU Matrices	$(MP, M, M^{N+1}P, M^{N+1})$	$M \geq 2, P > 0$	$\surd$	Indirect
[28]	GCP	(rZ, L, rs, s)	$r, s \geq 2, s\|Z$	$\times$	Indirect
[29]	ZCP	$(2^m, 2^m, L, Z)$	$Z \geq \lceil \frac{L}{2} \rceil$	$\surd$	Direct
[30]	PBF	$(\prod_{i=1}^{l} p_i 2^{n+1}, 2^{n+1}, 2^m \prod_{i=1}^{l} p_i, 2^m)$	$\forall p_i$ is a prime	$\times$	Direct
[31]	PBF	$(p2^{k+1}, 2^{k+1}, p2^m, 2^m)$	p is a prime	$\surd$	Direct
Theorem 3.3	EBF	$(q^{v+d}, q^d, q^m, q^{m-v})$	$v < m$	$\surd$	Direct

From Table 1, we know that all the constructions of MOCSs based on generalized Boolean functions have length with the form of 2^m or $2^m + 2^t$ [25,26,32,33]. Certainly, there are also some other sporadic constructions of MOCSs. For example, some researchers design MOCSs by paraunitary (PU) matrice [34,35], even-shift complementary sequence sets (ESCSSs) or CCCs [36], multivariable functions, kronecker product and extended Boolean functions [22]. However, some MOCSs are relatively simple in length. Compared with the previous constructions, our designs are available for arbitrary integer q. In addition, our first MOCSs which have certain lengths can also be regarded as CCCs and our second MOCSs has the advantage of flexible lengths than before.

From Table 2, we see that some constructions of ZCCSs are mainly based on generalized Boolean functions [17–21]. As for other methods, some researchers provided ZCCSs by Z-paraunitary (ZPU) matrices [27], GCP, Z-complementary pair (ZCP), unitary matrices [28, 29], Pseudo-Boolean functions (PBF) [30,31] and extended Boolean functions [22]. However, the parameters of the known direct constructions of ZCCSs based on GBFs are mostly related to 2 and only [22] breaks through this limitation by utilizing the arbitrariness of q. Compared with [22], our construction can accommodate more users on the basis of achieving the optimality.

6 Conclusion

In this paper, we mainly present a constructions of optimal ZCCSs and a construction of MOCSs with flexible lengths. All these designs are based on EBFs. Compared with the previous works, especially the recent work by Shen et al. [22], we show that our construction can generate MOCSs and ZCCSs consisting of sequences with new parameters which have not been reported before. Not only that, by assigning different values to q, a wide range of q-ary MOCSs and ZCCSs can be obtained. One highlight of this paper is our designation of MOCSs with flexible lengths, due to its good correlation properties and the variable-lengths, it may have many applications in wireless communication.

Declarations

Funding This research was supported by the National Natural Science Foundation of China (Grant No. 12171241)

Conficts of interest The authors declare that they have no conficts of interest.

Ethics approval and consent to participate Not applicable.

Consent for publication Not applicable.

References

[1] Golay M.J.E.: Complementary series. IEEE Trans. Inf. Theory. **7**(2), 82-87 (1987).

[2] Chen H.H., Yeh J.F., and Suehiro N.: A multicarrier CDMA architecture based on orthogonal complete complementary codes for new generations of wideband wireless communications. IEEE Commun. Mag. **39**, 126-134 (2001).

[3] Welti G.R.: Quaternary codes for pulsed radar. IEEE Trans. Inf. Theory. **6**(3), 400-40 (1960).

[4] Tasinkevych Y., Trots I., and Nowicki A.: Mutually orthogonal Golay complementary sequences in the simultaneous synthetic aperture method for medical ultrasound diagnostics. Ultrasonics. **115** (2021).

[5] Spasojevic P., and Georghiades C.N.: Complementary sequences for ISI channel estimation. IEEE Trans. Inf. Theory. **47**(3), 1145-1152 (2001).

[6] Paterson K.G.: Generalized Reed-Muller codes and power control in OFDM modulation. IEEE Trans. Inf. Theory. **46**(1), 104-120 (2000).

[7] Tseng C.C. and Liu C.: Complementary sets of sequences. IEEE Trans. Inf. Theory. **18**(5), 644-652 (1972).

[8] Chen C.: A novel construction of complementary sets with flexible lengths based on Boolean functions. IEEE Commun. Lett. **22**(2), 260-263 (2018).

[9] Chen C.: A new construction of Golay complementary sets of non-power-of-two length based on Boolean functions. In Proc. IEEE Wireless Commun. Netw. Conf. 1-6 (2017).

[10] Wang Z., Xue E., and Chai J.: A method to construct complementary sets of non-power-of-two length by concatenation. In Proc. 8th Int. Workshop Signal Design Appl. Commun (IWSDA), Sapporo, Japan. 24-28 (2017).

[11] Suehiro N., and Hatori M.: N-shift cross-orthogonal sequences. IEEE Trans. Inf. Theory. **34**(1), 143-146 (1988).

[12] Zhang Z., Tian F., Zeng F., Ge L., and Xuan G.: Mutually orthogonal complementary pairs for OFDM-CDMA systems. 12th Int. conf. Signal Process, HangZhou. 1761-1765 (2014).

[13] Aparicio J., and Shimura T.: Asynchronous detection and identification of multiple users by multi-carrier modulated complementary set of sequences. IEEE Access. **6**, 22054-22069 (2018).

[14] Liu Z., Guan Y.L., and Parampalli U.: New complete complementary codes for peak-to-mean power control in multi-carrier CDMA. IEEE Trans. Commun. **62**(3), 1105-1113 (2014).

[15] Tseng S.M. and Bell M.R.: Asynchronous multicarrier DS-CDMA using mutually orthogonal complementary sets of sequences," IEEE Trans. Commun. **48**(1), 53-59 (2000).

[16] Fan P., Yuan W., and Tu Y.: Z-complementary binary sequences. IEEE Signal Process. Lett. **14**(8), 509-512 (2007).

[17] Sarkar P., Roy A., and Majhi S.: Construction of Z-complementary code sets with non-power-of-two lengths based on generalized Boolean functions. IEEE Commun. Lett. **24**(8), 1607-1611 (2020).

[18] Sarkar P., and Majhi S.: A direct construction of optimal ZCCS with maximum column sequence PMEPR two for MC-CDMA system. IEEE Commun. Lett. **25**(2), 337-341 (2021).

[19] Sarkar P., Majhi S., and Liu Z.: Optimal Z-complementary code set from generalized Reed-Muller Codes. IEEE Trans. Commun. **67**(3), 1783-1796 (2019).

[20] Wu S., and Chen C.: Optimal Z-complementary sequence sets with good peak-to-average power-ratio property. IEEE Signal Process. Lett. **25**(10), 1500-1504 (2018).

[21] Xie C., Sun Y., and Ming Y.: Constructions of optimal binary Z-complementary sequence sets with large zero correlation zone. IEEE Signal Process. Lett. **28**, 1694-1698 (2021).

[22] Shen, B., Meng, H., Yang, Y. et al. New constructions of Z-complementary code sets and mutually orthogonal complementary sequence sets. Des. Codes Cryptogr. (2022). https://doi.org/10.1007/s10623-022-01112-5

[23] Feng L., Fan P., and Zhou X.: Lower bounds on correlation of Z-complementary code sets. Wirel. Pers. Commun. **72**(2), 1475-1488 (2013).

[24] Chen C.: Complementary sets of non-power-of-two length for peak-to-average power ratio reduction in OFDM. IEEE Trans. Inf. Theory. **62**(12), 7538-7545 (2016).

[25] Wu S., Chen C., and Li Z.: How to construct mutually orthogonal complementary sets with non-power-of-two lengths?. IEEE Trans. Inf. Theory. **67**(6), 3464-3472 (2021).

[26] Rathinakumar A., and Chaturvedi A.K.: Complete mutually orthogonal golay complementary sets from reed-muller codes. IEEE Trans. Inf. Theory. **54**(3), 1339-1346 (2008).

[27] Das S., Parampalli U., Majhi S., Liu Z., and S. Budišin.: New optimal Z-complementary code sets based on generalized paraunitary matrices. IEEE Trans. Commun. **68**, 5546-5558 (2020).

[28] Li Y., and Xu C.: ZCZ aperiodic complementary sequence sets with low column sequence PMEPR. IEEE Commun. Lett. **19**(8), 1303-1306 (2015).

[29] Adhikary A. R., and Majhi S.: New construction of optimal aperiodic Z-complementary sequence sets of odd-lengths. Electronics Lett. **55**(19), 1043-1045 (2019).

[30] Ghosh G., Sudhan M., Palash S., and Ashish K.U.: Direct construction of optimal Z-complementary code sets for all possible even length by using pseudo-Boolean functions. arXiv:2108.02689. (2021).

[31] Sarkar P., Majhi S., and Liu Z.: Pseudo-Boolean functions for optimal Z-complementary code sets with flexible lengths. IEEE Signal Process. Lett. **28**, 1350-1354 (2021).

[32] Chen C., Wang C.H., and Chao C.C.: Complete complementary codes and generalized reed-muller codes. IEEE Commun. Lett. **12**(11), 849-851 (2008).

[33] Tian L., Lu X., Xu C., and Li Y.: New mutually orthogonal complementary sets with non-power-of-two lengths. IEEE Commun. Lett. **28**, 359-363 (2021).

[34] Das S., Budišin S., Majhi S., Liu Z., and Guan Y.L. : A multiplier-free generator for polyphase complete complementary codes. IEEE Trans. Signal Process. **66**(5), 1184-1196 (2018).

[35] Das S., Majhi S., and Liu Z.: A novel class of complete complementary codes and their applications for APU matrices. IEEE Signal Process. Lett. **25**(9), 1300-1304 (2018).

[36] Shen B., Yang Y., and Zhou Z.: A generalised construction of mutually orthogonal complementary sequence sets with non-power-of-two lengths. IEEE Trans. Commun. **69**(7), 4247-4253 (2021).

[37] Sarkar P., Liu Z., and Majhi S.: Multivariable function for new complete complementary codes with arbitrary lengths. arXiv:2102.10517. (2021).

[38] Kumar P., Majhi S., and Paul S.: A Direct Construction of GCP and Binary CCC of Length Non Power of Two. arXiv:2109.08567. (2021).

[39] Ma D., Budišin S., Wang Z. and Gong G.: A New Generalized Paraunitary Generator for Complementary Sets and Complete Complementary Codes of Size 2^m. IEEE Signal Process. Lett. **26**(1), 4-8 (2019).

[40] Jin Y., and Koga H.: Basic properties of the complete complementary codes using the DFT matrices and the Kronecker products. In Proc. 2008 International Symp. Inf. Theory and Its Appl. 1-6 (2008).

[41] Gu Z., Zhou Z., Adhikary A., Feng Y., and Fan P.: Asymptotically optimal Golay-ZCZ sequence sets with flexible length. arXiv:2112.08678. (2021).