Two Novel Constructions of Mutually Orthogonal Complementary Sets

Yu Wang[1], Dejiao Cai[1], Yongqiu Chen[1], Zilong Liu[2], Chunlei Li[3], Xiuping Peng[1]
[1]School of Information Science and Engineering, Yanshan University, Qinhuangdao, 066004, Hebei, China
Email: w301yu@163.com; 3181885479@qq.com; 845235798@qq.com; pengxp@ysu.edu.cn
[2]School of Computer Science and Electronic Engineering, University of Essex, United Kingdom
Email:zilong.liu@essex.ac.uk
[3]Department of Informatics, University of Bergen, 5020 Bergen, Norway
Email:chunlei.li@uib.no

***Abstract*—This paper presents two new constructions of mutually orthogonal complementary sets (MOCSs), which have found wide applications in engineering. The first is a direct method utilizing extended generalized Boolean functions (EGBFs) to generate MOCSs with flexible, non-power-of-two lengths. This method can also produce complete complementary codes (CCCs) and is well-suited for hardware implementation. The second is an indirect method that combines existing complementary sequence sets (CSSs) and MOCSs to create larger sets. To further expand the existence space of MOCSs, we also propose a novel direct construction method for CSSs.**

***Index Terms*—Multi-carrier code division multiple access (MC-CDMA), Mutually orthogonal complementary sets (MOCSs), Extended generalized Boolean functions (EGBFs)**

I. Introduction

An (M,N,L)-mutually orthogonal complementary set (MOCS) refers to M (N,L)- complementary sequence sets (CSSs), where any two distinct CSSs have zero cross-correlation sums at all time shifts [1]. Suehiro and Hatori showed that $M \leq N$ in [2], and when the equality is met, it is called a set of (M,L)-complete complementary codes (CCCs). Owing to the ideal auto-correlation and cross-correlation properties, CCCs and MOCSs are useful for a wide range of applications, including synthetic aperture imaging systems [3] and orthogonal frequency division multiplexing-code division multiple access (OFDM-CDMA) systems [4]. MOCSs can be used to eliminate both multi-user interference (MUI) and multi-path interference (MPI), making them particularly effective in multi-carrier code division multiple access (MC-CDMA) systems [5] and massive multiple-input multiple-output (MIMO) communication systems for applications like channel estimation [6] and cell search [7].

The construction methods of MOCSs can be broadly categorized into two types: direct construction, which often uses mathematical tools such as Boolean functions (BFs) and multi-variable functions (MVFs), and indirect constructions, which utilize techniques such as the Kronecker product, interleaving and paraunitary (PU) matrices. Davis and Jedwab proposed the direct construction of Golay complementary pairs (GCPs) with length 2^m $(m > 2)$ using generalized Boolean functions (GBFs) in [8]. In [9], Paterson linked even q-ary GCPs with second-order GBFs based on the method of Davis and Jedwab. Moreover, direct constructions of q-ary MOCSs with flexible non-power-of-two lengths were developed [11], [12]. In [12], Sarkar et al. proposed q-ary (p^{n+1}, p^m)-CCCs, where p is a prime number and q is a positive integer multiple of p, but the sequence lengths of the constructed CCCs only exists in the form of prime power.

Recently, a new construction of $(q^{d'}, q^{v+d}, \gamma)$-MOCSs with flexible lengths has been proposed in [13] based on extended Boolean functions (EBFs), where $\gamma = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u$, $0 < d' < d < m$, $0 < v < m$, $a_k \in \mathbb{Z}_q, a_m \in \mathbb{Z}_q^*$ and q are positive integers no less than 2. However, since $d' < d$ and v are positive integers, the number of sequences q^{v+d} in each set is at least (when $v = 1$) q^2 times the number of sets $q^{d'}$ in the MOCSs, resulting in certain gaps in the set sizes. In addition, some indirect construction methods are also provided in [14]–[20], which require complex calculations and are not suitable for hardware generation. In [18]–[20], Das et al. proposed methods of constructing CCCs and MOCSs of distinct lengths using PU matrices. It should be noted that the construction of MOCSs based on PU matrices is not as straightforward as that based on GBFs.In [21], [22], Wang et al. intensively investigated the PU matrix construction.

Building upon prior research on MOCSs, this paper first presents a new construction of q-ary $(b^k, b^{k+v}, \eta \cdot b^{m-1})$-MOCSs based on extended generalized Boolean functions (EGBFs), where $k \leq m-v$, $v < m$, $b|q$ and $b \geq 2$, $\eta \in \mathbb{N}_b$. Our proposed MOCSs have flexible and variable lengths, thus filling some gaps with respect to the results in [13]. It should be noted that by limiting the values of certain parameters, this construction also yields (b^k, b^m)-CCCs. In addition, we present a direct construction of CSSs based on EGBFs. With the aid of the Kronecker product and by using (K, L_1)-CSSs and (M,N,L_2)-MOCSs as basic sequences, another construction of (M, NK, L_1L_2)-MOCSs is further proposed.

The work of Xiuping Peng was supported in part by Hebei Natural Science Foundation under Grant F2025203049 and in part by S&T Program of HeBei under Grant 236Z0403G. The work of Z. Liu was supported in part by the UK Engineering and Physical Sciences Research Council under grant EP/Y000986/1 ('SORT'), by the Royal Society under Grants IEC\R3\223079 and IES\R1\241212, and by the British Council under Grant UKIERI-SPARC/01/22.

II. Preliminaries

First, some symbols that will be used throughout the paper are presented as: $\xi = e^{2\pi\sqrt{-1}/q}$ denotes the q-th roots of unity; $\boldsymbol{x} = (x_0, x_1, ..., x_{L-1})$ refers to a sequence of length L; $\mathbb{Z}_q = \{0, 1, ..., q-1\}$ is the ring of the integers modulo q, and $\mathbb{Z}_q^* = \mathbb{Z}_q \backslash \{0\}$; $\mathbb{N}_t = \{1, 2, ..., t\}$ denotes the set of positive integers from 1 to t; $\lfloor a \rfloor$ is the largest integer less than or equal to a; $b|q$ denotes that b divides q; $\boldsymbol{x} \oplus a = (x_0 \oplus a, x_1 \oplus a, ..., x_{L-1} \oplus a)$, where $\oplus$ denotes the element-wise addition at corresponding positions; $(\cdot)^*$ refers to the conjugate of $(\cdot)$; $\mathscr{U}(b) \triangleq \{t : \gcd(b,t) = 1\}$, where $t \in \{1, 2, ..., b-1\}$; $\otimes$ denotes the Kronecker product.

Definition 1. Assume that $\boldsymbol{a} = (a_0, a_1, ..., a_{L-1})$ and $\boldsymbol{b} = (b_0, b_1, ..., b_{L-1})$ are $\mathbb{Z}q$-valued sequences of length L. The aperiodic cross-correlation function (ACCF) $R_{\boldsymbol{a},\boldsymbol{b}}(\tau)$ between $\boldsymbol{a}$ and $\boldsymbol{b}$ at τ is defined as follows:

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

When $\boldsymbol{a} = \boldsymbol{b}$, $R_{\boldsymbol{a}}(\tau)$ is referred to as the AACF. Given the definition above, it is easy to derive that $R_{\boldsymbol{b},\boldsymbol{a}}(-\tau) = R^*_{\boldsymbol{a},\boldsymbol{b}}(\tau)$.

Definition 2. The set $G = \{\boldsymbol{g}_0, \boldsymbol{g}_1, ..., \boldsymbol{g}_{N-1}\}$ composed of N sequences, each of length L, is called a complementary sequence set, denoted as (N,L)-CSS, if for all $\tau \neq 0$, $R_G(\tau) = \sum_{i=0}^{N-1} R_{\boldsymbol{g}_i}(\tau) = 0$ holds.

Definition 3. A set $\mathscr{G} = \{G^0, G^1, ..., G^{M-1}\}$ consisting of M sequence sets is referred to as an (M,N,L) -MOCS if the following conditions are met:

$$R_{G^i,G^j}(\tau) = \sum_{k=0}^{N-1} R_{\boldsymbol{g}_k^i, \boldsymbol{g}_k^j}(\tau) = \begin{cases} NL & \tau = 0, i = j \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Any sequence set $G^m = \{\boldsymbol{g}_0^m, \boldsymbol{g}_1^m, ..., \boldsymbol{g}_{N-1}^m\}$ in $\mathscr{G}$ is clearly a CSS, where $0 \le m \le M-1$.

Lemma 1. [2] For an (M,N,L)-MOCS, the upper bound of the set size satisfies $M \le N$. When the equality holds, it is denoted as (M,L)-CCC.

EGBFs $f : \mathbb{Z}_b^m \to \mathbb{Z}_q$ involves m variables $x_1, x_2, \ldots, x_m$, where $x_i \in \mathbb{Z}_b$ for $i = 1, 2, \ldots, m$, and $b \mid q$. A degree-d monomial is defined as the product of d distinct variables. For example, $x_1x_2x_3$ is a degree-3 monomial. The sequence $\boldsymbol{f}$ associated with the function f over m variables is defined as $\boldsymbol{f} = (f_0, f_1, \ldots, f_{b^m-1})$, where $f_i = f(i_1, i_2, \ldots, i_m)$, and $(i_1, i_2, \ldots, i_m)$ corresponds to the b-ary representation of the integer $i = \sum_{k=1}^m i_k b^{k-1}$.

III. Main works

A. A Direction Construction of MOCSs

Theorem 1. Let m, k, v, b, q be non-negative integers such that $k \le m - v$, $v < m$, $b \ge 2$, and $b|q$. Assume that $\{I_1, I_2, \ldots, I_k\}$ be a partition of the set $\mathbb{N}_{m-v}$, π_α is a permutation from $\mathbb{N}_{m_\alpha}$ to I_α, where $\alpha \in \mathbb{N}_k$, $|I_\alpha| = m_\alpha$. Define the EGBFs $f : \mathbb{Z}_b^m \to \mathbb{Z}_q$ as follows:

$$f(x) = \frac{q}{b} \sum_{\alpha=1}^{k} \sum_{\beta=1}^{m_\alpha - 1} d_{\alpha,\beta} x_{\pi_\alpha(\beta)} x_{\pi_\alpha(\beta+1)} + \sum_{s=1}^{q-1} \sum_{i=1}^{m} p_{i,s} x_i^s + p_0 \tag{3}$$

where $d_{\alpha,\beta} \in \mathscr{U}(b)$, $x_i \in \mathbb{Z}_b$, and $p_{i,s}, p_0 \in \mathbb{Z}_q$. Then define

$$\begin{aligned} g_n^r(x) = f(x) &+ \frac{q}{b} \sum_{\alpha=1}^{k} n_\alpha x_{\pi_\alpha(1)} + \frac{q}{b} \sum_{\mu=1}^{v} d_\mu n_{k+\mu} x_{m-v+\mu} \\ &+ \frac{q}{b} \sum_{\alpha=1}^{k} d_\alpha r_\alpha x_{\pi_\alpha(m_\alpha)} \end{aligned} \tag{4}$$

where $(r_1, r_2, \ldots, r_k)$ and $(n_1, n_2, \ldots, n_{k+v})$ are the b-ary representations of r and n, respectively, $d_\alpha, d_\mu \in \mathscr{U}(b)$. Then, $\mathscr{G} = \{G^0, G^1, \ldots, G^{b^k-1}\}$ forms an $(b^k, b^{k+v}, \eta \cdot b^{m-1})$-MOCS, where $\eta \in \mathbb{N}_b$, and $G^r = \{\mathbf{g}_0^r, \mathbf{g}_1^r, \ldots, \mathbf{g}_{b^{k+v}-1}^r\}$.

Proof. Part 1: Let $\mathbf{g}_n^r = (g_{n,0}^r, \ldots, g_{n,b^{k+v}-1}^r)$. It suffices to show that for any two sets G^{r_1} and G^{r_2}, the cross-correlation satisfies:

$$\begin{aligned} R_{G^{r_1},G^{r_2}}(\tau) &= \sum_{n=0}^{b^{k+v}-1} R_{\mathbf{g}_n^{r_1}, \mathbf{g}_n^{r_2}}(\tau) \\ &= \sum_{i=0}^{L-\tau-1} \sum_{n=0}^{b^{k+v}-1} \xi^{g_{n,i}^{r_1} - g_{n,i+\tau}^{r_2}} = 0 \end{aligned} \tag{5}$$

where $0 \le r_1, r_2 \le b^k - 1$, $L = \eta \cdot b^{m-1}$, and $0 < |\tau| \le L - 1$. For an arbitrary integer i, let $j = i + \tau$. Let $(i_1, i_2, \ldots, i_m)$ and $(j_1, j_2, \ldots, j_m)$ denote the b-ary representations of i and j, respectively.

Case 1: Assume that for some $\alpha \in \{1, 2, \ldots, k\}$, $i_{\pi_\alpha(1)} \neq j_{\pi_\alpha(1)}$, or for some $\mu \in \{1, 2, \ldots, v\}$, $i_{m-v+\mu} \neq j_{m-v+\mu}$. From (5), we derive

$$R_{G^{r_1},G^{r_2}}(\tau) = \sum_{i=0}^{L-\tau-1} \xi^{f_i - f_j} \cdot A \cdot B \cdot C = 0 \tag{6}$$

where $A = \prod_{\alpha=1}^{k} \left(\sum_{n_\alpha=0}^{b-1} \xi^{n_\alpha (i_{\pi_\alpha(1)} - j_{\pi_\alpha(1)})} \right), B = \prod_{\alpha=1}^{k} \xi^{r_{1\alpha} i_{\pi_\alpha(m_\alpha)} - r_{2\alpha} j_{\pi_\alpha(m_\alpha)}}, C = \prod_{\mu=1}^{v} \left(\sum_{n_{\mu+k}=0}^{b-1} \xi^{n_{\mu+k}(i_{m-v+\mu} - j_{m-v+\mu})} \right)$.

Case 2: Assume that $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ and $i_{m-v+\mu} = j_{m-v+\mu}$ hold for all $\alpha \in \{1, 2, \ldots, k\}$ and $\mu \in \{1, 2, \ldots, v\}$. When $i_m = j_m = 0$, we have

$$R_{G^{r_1},G^{r_2}}(\tau) = b^{k+v} \sum_{l=0}^{L-\tau-1} \xi^{f_i - f_j} \prod_{\alpha=1}^{k} \xi^{r_{1\alpha} i_{\pi_\alpha(m_\alpha)} - r_{2\alpha} j_{\pi_\alpha(m_\alpha)}} \tag{7}$$

Let α' be the largest integer such that $i_{\pi_\alpha(\beta)} = j_{\pi_\alpha(\beta)}$ for all $\alpha = 1, 2, \ldots, \alpha' - 1$ and $\beta = 1, 2, \ldots, m_\alpha$, and β' be the smallest integer satisfying $i_{\pi_{\alpha'}(\beta')} \neq j_{\pi_{\alpha'}(\beta')}$. Let i^h and j^h be integers differing from i and j only at position $\pi_{\alpha'}(\beta' - 1)$, specifically, $i^h_{\pi_{\alpha'}(\beta'-1)} = h \oplus i_{\pi_{\alpha'}(\beta'-1)}$, $j^h_{\pi_{\alpha'}(\beta'-1)} = h \oplus j_{\pi_{\alpha'}(\beta'-1)}$, where $1 \le h \le b - 1$. Consequently, we derive

$$f_{i^h} - f_i - (f_{j^h} - f_i) = h d_{\alpha',\beta'-1} (i_{\pi_{\alpha'}(\beta')} - j_{\pi_{\alpha'}(\beta')}) \tag{8}$$

Since $d_{\alpha',\beta'} \in \mathscr{U}(b)$, it follows that

$$\xi^{f_i - f_j} + \sum_{h=1}^{b-1} \xi^{f_{i^h} - f_{j^h}} = 0 \tag{9}$$

Combining (7) and (9), we have $R_{G^{r_1},G^{r_2}}(\tau) = 0$.

Case 3: Assume similarly that $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ and $i_{m-v+\mu} = j_{m-v+\mu}$ for all $\alpha \in \{1,2,\ldots,k\}$ and $\mu \in \{1,2,\ldots,v\}$. When $i_m = j_m = \eta \neq 0$, let α' be the largest integer such that $i_{\pi_\alpha(\beta)} = j_{\pi_\alpha(\beta)}$ for all $\alpha = 1,2,\ldots,\alpha'-1$ and $\beta = 1,2,\ldots,m_\alpha$, and β' denotes the smallest integer satisfying $i_{\pi_{\alpha'}(\beta')} \neq j_{\pi_{\alpha'}(\beta')}$. Let i^h and j^h as integers differing from i and j only at position $\pi_{\alpha'}(\beta'-1)$, where $1 \leq h \leq b-1$. Since $\pi_{\alpha'}(\beta') < m-v+\mu$, it follows that $\pi_{\alpha'}(\beta'-1) < m-v+\mu$, implying $i_{\pi_{\alpha'}(\beta'-1)} < i_m = \eta$ and similarly $j_{\pi_{\alpha'}(\beta'-1)} < \eta$. Thus, $i^h, j^h < \partial \cdot b^{m-1} = L$. Following an analogous argument to Case 2, we obtain:

$$\xi^{f_i - f_j} + \sum_{h=1}^{b-1} \xi^{f_{i^h} - f_{j^h}} = 0 \tag{10}$$

Combining all three cases above, we conclude that (5) holds for $0 < \tau \leq L-1$.

Part 2: Next, we prove that for any two distinct sets G^{r_1} and G^{r_2} when $0 \leq r_1 \neq r_2 \leq b^k - 1$, have

$$R_{G^{r_1},G^{r_2}}(0) = \sum_{n=0}^{b^{k+v}-1} \sum_{i=0}^{L-1} \xi^{g^{r_1}_{n,i} - g^{r_2}_{n,i}} = 0 \tag{11}$$

Since $r_1 \neq r_2$, there exists a minimal integer $\kappa \in \{1,2,\ldots,k\}$ such that $r_{1,\kappa} \neq r_{2,\kappa}$. Analogous to Case 2, for any integer $0 \leq i \leq L-1$, define i^h as differing from i only at position κ, i.e., $(i_1, i_2, \ldots, i_{\kappa-1}, i_\kappa \oplus h, i_{\kappa+1}, \ldots, i_m)$, where $1 \leq h \leq b-1$. Given that $d_k \in \mathscr{U}(b)$, we have:

$$\begin{aligned} &\xi^{g^{r_1}_{n,i} - g^{r_2}_{n,i}} + \sum_{h=1}^{b-1} \xi^{g^{r_1}_{n,i^h} - g^{r_2}_{n,i^h}} \\ =&\xi^{g^{r_1}_{n,i} - g^{r_2}_{n,i}} + \sum_{h=1}^{b-1} \xi_b^{h d_\kappa (r_{1\kappa} - r_{2\kappa})} = 0. \end{aligned} \tag{12}$$

Obviously, we get that

$$R_{G^{r_1},G^{r_2}}(0) = \sum_{n=0}^{b^{k+v}-1} \sum_{i=0}^{L-1} \xi^{g^{r_1}_{n,i} - g^{r_2}_{n,i}} = 0 \tag{13}$$

Combining the above two parts, Theorem 1 is proved. □

Remark 1. In Theorem 1, by setting different values for the parameters b, k and v, a highly flexible range of set sizes and sequence counts can be obtained. Moreover, when the set size and sequence count are b^k and b^{k+v} respectively, the constructed MOCSs can generate flexible sequence lengths based on the value of η. These further extend the existence space of MOCSs. It is worth mentioning that when the parameters $v = 0$ and $\eta = b$, $(b^k, b^{k+v}, \eta \cdot b^{m-1})$-MOCSs can be enhanced to (b^k, b^m)-CCCs.

Example 1. Setting $q = 6$, $b = 3$, $m = 4$, $v = k = 1$, $m_1 = 3$, $\eta = 2$, $r_0 = 0$, $d_{1,1}, d_{1,2} = 2$, $d_1 = 1$, $(\pi_1(1), \pi_1(2), \pi_1(3)) = (2,1,3)$, $(p_{1,1}, p_{2,1}, p_{3,1}, p_{4,1}, p_{5,1}) = (0,0,3,3,5)$, $(p_{1,2}, p_{2,2}, p_{3,2}, p_{4,2}, p_{5,2}) = (4,4,1,4,5)$, $(p_{1,3}, p_{2,3}, p_{3,3}, p_{4,3}, p_{5,3}) = (5,0,3,1,0)$ and $(p_{1,4}, p_{2,4}, p_{3,4}, p_{4,4}, p_{5,4}) = (4,0,4,4,2)$ in Theorem 1. Then a $(3,9,54)$-MOCS $\mathscr{G} = \{G^0, G^1, G^2\}$ can be obtained, and this MOCS is a new set with parameters that have not been proposed in existing results. G^0,G^1 and G^2 are given in Table I.

B. An Indirect Construction of MOCSs

Theorem 2. Let m, b, k be non-negative integers with $b \geq 2$ and $k \leq m$. Let π be a permutation of the set $\{1,2,\ldots,m\}$. Define EGBFs $f : \mathbb{Z}_b^m \to \mathbb{Z}_q$ as follows:

$$f(x) = \frac{q}{b}\left(\sum_{\alpha=1}^{m-1} x_{\pi(\alpha)} x_{\pi(\alpha+1)} + x_{\pi(m)}\right) + \sum_{\mu=1}^{m} p_\mu x_\mu + p_0 \tag{14}$$

where $b \mid q$, $x_\mu \in \mathbb{Z}_b$, and $p_\mu, p_0 \in \mathbb{Z}_q$. Let

$$S = f(x) + \frac{q}{N} n_k x_{\pi(1)} + \frac{q}{N} \sum_{\alpha=1}^{k-1} n_\alpha x_{m-k+\alpha} \tag{15}$$

where $N \geq b$, $N \mid q$, and $n_k, n_\alpha \in \mathbb{Z}_N$. Then, $S = \{\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{N^k-1}\}$ forms a q-ary (N^k, b^m)-CSS.

Proof. By the definition of AACF, we have

$$R_S(\tau) = \sum_{n=0}^{N^k-1} \sum_{i=0}^{b^m-\tau-1} \xi^{s_{n,i} - s_{n,i+\tau}} \tag{16}$$

where $s_{n,i}$ denotes the i-th element of the sequence $\boldsymbol{s}_n$. For an arbitrary integer i, let $j = i + \tau$, and let $(i_1, i_2, \ldots, i_m)$ and $(j_1, j_2, \ldots, j_m)$ represent the b-ary representations of i and j, respectively.

Case 1: Assume $i_{\pi(1)} \neq j_{\pi(1)}$, or there exists an $\alpha \in \{1,2,\ldots,k-1\}$ such that $i_{m-k+\alpha} \neq j_{m-k+\alpha}$.The proof follows similar reasoning to that employed in Case 1 of Part 1 in the demonstration of Theorem 1.

Case 2: Assume $i_{\pi(1)} = j_{\pi(1)}$, and $i_{m-k+\alpha} = j_{m-k+\alpha}$ for all $\alpha \in \{1,2,\ldots,k-1\}$, then we have

$$R_S(\tau) = N^k \sum_{i=0}^{b^m-\tau-1} \xi^{f_i - f_j} \tag{17}$$

Let β denote the smallest integer such that $i_{\pi(\beta)} \neq j_{\pi(\beta)}$. Define i^h and j^h as integers differing from i and j only at position $\pi(\beta-1)$. From (14), we obtain

$$f_{i^h} - f_i - (f_{j^h} - f_j) = h\frac{q}{b}(i_{\pi(\beta)} - j_{\pi(\beta)}) \tag{18}$$

Further, we have

$$\xi^{f_i - f_j} + \sum_{h=1}^{b-1} \xi^{f_{i^h} - f_{j^h}} = \xi^{f_i - f_j} + \sum_{h=1}^{b-1} \xi^{h\frac{q}{b}(i_{\pi(\beta)} - j_{\pi(\beta)})} = 0 \tag{19}$$

From (17) and (19), it follows that

$$R_S(\tau) = 0 \tag{20}$$

In conclusion, we conclude that the set S forms a CSS. □

TABLE I
THE SPECIFIC NUMERICAL FORMS OF G^0, G^1 AND G^2

$\mathscr{G}$	Number Result
G^0	$\begin{pmatrix} 232343010325214325250523412505010343052541052523250145; 232505454325430103250145250505232121052103430523412523; \\ 232121232325052541250301034505454505052325214523034301; 232343010325214325250523412121232505214103214145412301; \\ 232505454325430103250145250121454343214325052145034145; 232121232325052541250301034121010121214541430145250523; \\ 232343010325214325250523412343454121430325430301034523; 232505454325430103250145250343010505430541214301250301; \\ 232121232325052541250301034343232343430103052301412145 \end{pmatrix}$
G^1	$\begin{pmatrix} 250301034343232343214541430523034301010505010541214103; 250523412343454121214103214523250145010121454541430541; \\ 250145250343010505214325052523412523010343232541052325; 250301034343232343214541430145250523232121232103430325; \\ 250523412343454121214103214145412301232343010103052103; 250145250343010505214325052145034145232505454103214541; \\ 250301034343232343214541430301412145454343454325052541; 250523412343454121214103214301034523454505232325214325; \\ 250145250343010505214325052301250301454121010325430103 \end{pmatrix}$
G^2	$\begin{pmatrix} 214325052301250301232505454541052325034523034505232121; 214541430301412145232121232541214103034145412505454505; \\ 214103214301034523232343010541430541034301250505010343; 214325052301250301232505454103214541250145250121454343; \\ 214541430301412145232121232103430325250301034121010121; 214103214301034523232343010103052103250523412121232505; \\ 214325052301250301232505454325430103412301412343010505; 214541430301412145232121232325052541412523250343232343; \\ 214103214301034523232343010325214325412145034343454121 \end{pmatrix}$

Lemma 2. [12] Let $(\boldsymbol{x}_1,\boldsymbol{x}_2)$ be two sequences of length L_1 and $(\boldsymbol{y}_1,\boldsymbol{y}_2)$ be two sequences of length L_2. Then aperiodic correlation of $\boldsymbol{x}_1\otimes\boldsymbol{y}_1$ and $\boldsymbol{x}_2\otimes\boldsymbol{y}_2$ is given by

$$\begin{aligned} R_{\boldsymbol{x}_1\otimes\boldsymbol{y}_1,\boldsymbol{x}_2\otimes\boldsymbol{y}_2}(\tau) &= R_{\boldsymbol{x}_1,\boldsymbol{x}_2}(k_1)R_{\boldsymbol{y}_1,\boldsymbol{y}_2}(k_2) \\ &\quad + R_{\boldsymbol{x}_1,\boldsymbol{x}_2}(k_1+1)R_{\boldsymbol{y}_1,\boldsymbol{y}_2}(k_2-L_2) \end{aligned} \tag{21}$$

where $\tau = k_1L_2+k_2$, and $\otimes$ denotes the Kronecker product.

Theorem 3. Let $S=\{\boldsymbol{s}_0,\boldsymbol{s}_1,\ldots,\boldsymbol{s}_{K-1}\}$ be a (K,L_1)-CSS, and let $\mathscr{G}=\{G^0,G^1,\ldots,G^{M-1}\}$ be an (M,N,L_2)-MOCS. Define $W^m=\{\boldsymbol{w}_0^m,\boldsymbol{w}_1^m,\ldots,\boldsymbol{w}_{NK-1}^m\}$ as follows:

$$W^m=\begin{bmatrix}\boldsymbol{w}_0^m\\ \boldsymbol{w}_1^m\\ \vdots\\ \boldsymbol{w}_{NK-1}^m\end{bmatrix}=\begin{bmatrix}\boldsymbol{s}_0\otimes G^m\\ \boldsymbol{s}_1\otimes G^m\\ \vdots\\ \boldsymbol{s}_{K-1}\otimes G^m\end{bmatrix}=\begin{bmatrix}\boldsymbol{s}_0\otimes\boldsymbol{g}_0^m\\ \vdots\\ \boldsymbol{s}_0\otimes\boldsymbol{g}_{N-1}^m\\ \boldsymbol{s}_1\otimes\boldsymbol{g}_1^m\\ \vdots\\ \boldsymbol{s}_1\otimes\boldsymbol{g}_{N-1}^m\\ \vdots\\ \boldsymbol{s}_{K-1}\otimes\boldsymbol{g}_0^m\\ \vdots\\ \boldsymbol{s}_{K-1}\otimes\boldsymbol{g}_{N-1}^m\end{bmatrix} \tag{22}$$

where $G^m=\{\boldsymbol{g}_0^m,\ldots,\boldsymbol{g}_{N-1}^m\}$ and $m=0,\ldots,M-1$. Then, $\mathscr{W}=\{W^0,\ldots,W^{M-1}\}$ forms an (M,NK,L,L_2)-MOCS.

Proof. First, we demonstrate that for $0\le m<M$, W^m forms a CSS of length L_1L_2.

By Lemma 2, we have

$$\begin{aligned} &\sum_{i=0}^{K-1} R_{\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_1}^m,\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_2}^m}(\tau_0) \\ &=\begin{cases} KL_1R_{\boldsymbol{g}_{n_1}^m,\boldsymbol{g}_{n_2}^m}(k_2), & k_2=0 \\ 0, & \text{otherwise} \end{cases} \end{aligned} \tag{23}$$

where $\tau_0=k_1L_2+k_2$. For W^m, considering $\tau=rL_1L_2+\tau_0$, it follows that

$$\begin{aligned} &\sum_{l=0}^{NK-1} R_{\boldsymbol{w}_l^m}(\tau) \\ &=\sum_{i=0}^{K-1}\sum_{n_1=0}^{N-1-r}\left(R_{\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_1}^m,\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_2}^m}(\tau_0)+R_{\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_1}^m,\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_2+1}^m}(\tau_0-L_1L_2)\right) \end{aligned} \tag{24}$$

where $n_2=n_1+r$.

Clearly, when $r\ge 1$, we obtain

$$\sum_{l=0}^{NK-1} R_{\boldsymbol{w}_l^m}(\tau)=0 \tag{25}$$

Consider $r=0$, then

$$\begin{aligned} \sum_{l=0}^{NK-1} R_{\boldsymbol{w}_l^m}(\tau) &= \sum_{i=0}^{K-1}\sum_{n_1=n_2=0}^{N-1} R_{\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_1}^m,\boldsymbol{s}_i\otimes\boldsymbol{g}_{n_2}^m}(\tau_0) \\ &=\begin{cases} KL_1\sum\limits_{n_1=n_2=0}^{N-1} R_{\boldsymbol{g}_{n_1}^m,\boldsymbol{g}_{n_2}^m}(k_2), & k_1=0 \\ 0, & k_1\ne 0 \end{cases} \\ &=\begin{cases} KNL_1L_2, & k_1=0,k_2=0 \\ 0, & \text{otherwise} \end{cases} \end{aligned} \tag{26}$$

Next, we show that for $m_1\ne m_2$, i.e., any two distinct sequence sets W^{m_1} and W^{m_2} are mutually orthogonal.

Considering the sum of cross-correlations between W^{m_1} and W^{m_2}, analogous to (24),(25) and (26), when $r\ge 1$ or $r=0$, we always can obtain $\sum_{l=0}^{NK-1}R_{\boldsymbol{w}_l^{m_1},\boldsymbol{w}_l^{m_2}}(\tau)=0$.

Combining all cases, Theorem 3 is proved. □

IV. COMPARISON

Previous methods for constructing MOCSs have significant limitations, as summarized in Table 1. Constructions based on GBFs for instance, are often restricted to sequence lengths that are powers of two or simple sums thereof [10], [11]. While other methods, like those in [12] and [13], offer more flexibility with non-power of two lengths, they still face constraints. Notably, the method in [13] introduces parameter gaps, where the number of sequences per set is at least q^2

TABLE II
PARAMETER COMPARISON OF EXISTING RESULTS FOR MOCSS

Ref.	Parameters	Conditions	Based on
[10]	$(2^k, 2^k, 2^m)$	$0 < k \leq m$	GBFs
[11]	$(2^{k'}, 2^{k+1}, 2^m + 2^t)$	$0 < k, t \leq m; 0 \leq k' \leq t; k' \leq k-1$	GBFs
[12]	(p^{n+1}, p^{n+1}, p^m)	prime p, $0 < n < m$	q-ary function
[18]	(M, M, N^m)	$N \mid M, m > 0$	PU matrix
[15]	(M, M, MN_1N_2)	(M, M, N_1)-CCC and (M, M, N_2)-CCC	Kronecker product
[17]	$(M_1M_2/2, M_1M_2/2, 2L_1L_2)$	even M_1, M_2, $L_1, L_2 \in \mathbb{N}^+$	Concatenation
[13]	$(q^{d'}, q^{v+d}, a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u)$	$0 < d' < d < m$, $a_k \in \mathbb{Z}_q$, $a_m \in \mathbb{Z}_q^*$, $q \geq 2$	EBFs
Theorem 1	$(b^k, b^{k+v}, \eta \cdot b^{m-1})$	$v < m, k \leq m - v$, $b \geq 2, b \mid q$, $\eta \in \mathbb{N}_b$	EGBFs
Theorem 3	(M, NK, L_1L_2)	(K, L_1)-CSS and (M, N, L_2)-MOCS	Kronecker product

times larger than the number of sets, limiting the flexibility of set sizes.

Our first method, detailed in Theorem 1, uses EGBFs to construct MOCSs with flexible set sizes and variable sequence lengths. This approach overcomes the parameter gaps found in [13]. Furthermore, by setting specific parameters (as shown in Remark 1), these MOCSs can be specialized to CCCs.

We introduce a novel indirect construction method in Theorem 3. Unlike previous indirect methods that use techniques like PU matrices [18], Kronecker products [15] or concatenation [17], our approach uses existing CSSs and MOCSs as building blocks with the Kronecker product. This expands the parameter space of MOCSs, particularly the number of sequences, beyond power-of-two forms. More specifically, by combining the MOCSs from Theorem 1 and the CSSs from Theorem 2, we can construct new MOCSs with parameters like $(b^k, N^k \cdot b^{k+v}, \eta \cdot b^{2m-1})$. This enables the creation of previously unattainable MOCSs, such as $(3, 12, L)$-MOCSs,where $L = \eta \cdot b^{2m-1}$ denotes the sequence lengths, and L can also take on flexible lengths based on the value of η.

V. CONCLUSION

In this work, we have introduced two novel methods for constructing MOCSs. The first is a direct method using EGBFs, which generates MOCSs with flexible set sizes and variable sequence lengths, addressing parameter gaps found in existing literature [13]. Under certain conditions, it has been shown that it leads to CCCs. We have also proposed a direct construction for CSSs where the number of sequences and their lengths are powers of different integers. Based on these newly constructed CSSs and MOCSs as building blocks and via the Kronecker product, the existence space of MOCSs has been significantly expanded.

REFERENCES

[1] C.-C. Tseng and C. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory*, vol. 18, no. 5, pp. 644–652, Sep. 1972.

[2] N. Suehiro and M. Hatori, "N-shift cross-orthogonal sequences," *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 143–146, Jan. 1988.

[3] Y. Tasinkevych, I. Trots, and A. Nowicki, "Mutually orthogonal Golay complementary sequences in the simultaneous synthetic aperture method for medical ultrasound diagnostics," *Ultrasonics*, vol. 115, pp. 106434, 2021.

[4] Z. Zhang, F. Tian, F. Zeng, L. Ge, and G. Xuan, "Mutually orthogonal complementary pairs for OFDM-CDMA systems," *12th Int. Conf. Signal Process. (ICSP)*, Hangzhou, pp. 1761–1765, 2014.

[5] Z. Liu, Y. L. Guan, and U. Parampalli, "New complete complementary codes for peak-to-mean power control in multi-carrier CDMA," *IEEE Trans. Commun.*, vol. 62, no. 21, pp. 1105–1113, Nov. 2014.

[6] S. Wang and A. Abdi, "MIMO ISI channel estimation using uncorrelated Golay complementary sets of polyphase sequences," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 3024–3039, Sep. 2007.

[7] C.-Y. Chen, Y.-J. Min, K.-Y. Lu, and C.-C. Chao, "Cell search for cell-based OFDM systems using quasi complete complementary codes," *IEEE Int. Conf. Commun.*, pp. 4840–4844, 2008.

[8] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, Nov. 1999.

[9] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104–120, Jan. 2000.

[10] A. Rathinakumar and A. K. Chaturvedi, "Complete mutually orthogonal Golay complementary sets from Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1339–1346, Mar. 2008.

[11] S.-W. Wu, C.-Y. Chen, and Z. Liu, "How to construct mutually orthogonal complementary sets with non-power-of-two lengths?," *IEEE Trans. Inf. Theory*, vol. 67, no. 6, pp. 3464–3472, Jun. 2021.

[12] P. Sarkar, C. Li, S. Majhi, and Z. Liu, "New correlation bound and construction of quasi-complementary sequence sets," *IEEE Trans. Inf. Theory*, vol. 70, no. 3, pp. 2201–2223, 2024.

[13] H. Xiao and X. Cao, "New constructions of mutually orthogonal complementary sets and Z-complementary code sets based on extended Boolean functions," *Cryptogr. Commun.*, vol. 16, pp. 167–184, 2024.

[14] Y. Jin and H. Koga, "Basic properties of the complete complementary codes using the DFT matrices and the Kronecker products," *Int. Symp. Inf. Theory Appl. (ISITA)*, pp. 1–6, 2008.

[15] Z. Gu et al., "Asymptotically optimal Golay-ZCZ sequence sets with flexible length," *Chin. J. Electron.*, vol. 32, no. 4, pp. 806–820, 2023.

[16] K. Liu, J. Liu, and J. Ni, "Generalized construction of Z-complementary code sets of odd length," *IEEE Signal Process. Lett.*, vol. 30, pp. 354–358, 2023.

[17] B. Shen, H. Meng, Y. Yang, and Z. Zhou, "New constructions of Z-complementary code sets and mutually orthogonal complementary sequence sets," *Des. Codes Cryptogr.*, vol. 91, pp. 353–371, 2023.

[18] S. Das, S. Majhi, and Z. Liu, "A novel class of complete complementary codes and their applications for APU matrices," *IEEE Signal Process. Lett.*, vol. 25, no. 9, pp. 1300–1304, Sep. 2018.

[19] S. Das et al., "A multiplier-free generator for polyphase complete complementary codes," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1184–1196, Mar. 2018.

[20] S. Das, S. Majhi, S. Budišin, and Z. Liu, "A new construction framework for polyphase complete complementary codes with various lengths," *IEEE Trans. Signal Process.*, vol. 67, no. 10, pp. 2639–2648, May 2019.

[21] Z. Wang and G. Gong, "Constructions of complementary sequence sets and complete complementary codes by ideal two-level autocorrelation sequences and permutation polynomials," *IEEE Trans. Inf. Theory*, vol. 69, no. 7, pp. 4723–4739, 2023.

[22] Z. Wang, D. Ma, G. Gong, and E. Xue, "New construction of complementary sequence (or array) sets and complete complementary codes," *IEEE Trans. Inf. Theory*, vol. 67, no. 7, pp. 4902–4928, 2021.