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

Hongyang Xiao*, Xiwang Cao†

Abstract

Mutually orthogonal complementary sets (MOCSs) and Z-complementary code sets (ZCCSs) have many applications in practical scenarios such as synthetic aperture imaging systems and multi-carrier code division multiple access (MC-CDMA) systems. With the aid of extended Boolean functions (EBFs), in this paper, we first propose a direct construction of MOCSs with flexible lengths, and then propose a new construction of ZCCSs. The proposed MOCSs cover many existing lengths and have non-power-of-two lengths when $q = 2$. Our presented second construction can generate optimal ZCCSs meeting the set size upper bound. Note that the proposed two constructions are direct without the aid of any special sequence, which is suitable for rapid hardware generation.

Keywords: Multi-carrier code division multiple access (MC-CDMA)· mutually orthogonal complementary set (MOCS)· Z-complementary code set (ZCCS)· extended Boolean function (EBF).

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

1 Introduction

The concept of Golay complementary pair (GCP) was initiated by Golay in 1961 [?]. The aperiodic auto-correlation function (AACF) of a GCP diminishes to zero for all time shifts except at zero. In 1972, Tseng and Liu generalized the concept of GCP to Golay complementary sets (GCSs) and MOCSs [?]. An (N, L)-GCS is a set of N (≥ 2) sequences of

---

*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 Modeling and High Performance Computing of Air Vehicles (NUAA), MIIT, Nanjing, 211106, China, xwcao@nuaa.edu.cn

length L with the property that their AACF is zero for any non-zero time shifts and an (M, N, L)-MOCS is a collection of M GCSs, in which every GCS has N sequences of length L such that any two distinct GCSs are orthogonal. In 1988, Suehiro and Hatori proposed the concept of (N, N, L)-complete complementary codes (CCCs) whose set size achieves the theoretical upper bound of MOCSs (i.e., $M \leq N$) [?]. Due to the ideal correlation properties, MOCSs have been applied in many practical scenarios such as synthetic aperture imaging systems [?], OFDM-CDMA systems [?] and MC-CDMA systems [?, ?, ?].

In recent years, the construction of MOCSs has attracted extensive attention in sequence design community. Generalized Boolean functions (GBFs), usually are utilized to construct MOCSs. This is initiated by the pioneer work of Davis and Jedwab in [?] which proposed a direct construction of 2^h-ary $(h > 0)$ GCPs of length 2^m $(m > 0)$. Paterson extended the idea of [?] to construct q-ary (for even q) GCPs [?]. Further constructions of GCPs and GCSs based on GBFs have been proposed in [?, ?]. In [?], Tathinakumar and Chaturvedi proposed a direct construction of q-ary CCCs of length 2^m by extending Paterson's idea in [?]. Wu et $al.$ [?] designed MOCSs with non-power-of-two lengths. Later, a number of direct constructions of q-ary MOCSs with non-power-of-two lengths are presented in [?, ?]. Sarkar et $al.$ in [?] proposed (p^{n+1}, p^{n+1}, p^m)-CCCs via q-ary functions $(\mathbb{Z}_p^m \rightarrow \mathbb{Z}_q)$, where p is a prime number and q is a positive multiple of p. But these CCCs only have prime power lengths. In [?], Sarkar et $al.$ designed CCCs of length $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ (where each p_i is a prime and m_i is a positive integer) using multivariable functions (MVFs) [?]. This direct construction can generate q-ary CCCs of all possible lengths. However, in the case of $q = 2$, only binary CCC of length of form 2^m $(m \in \mathbb{Z})$ has been constructed [?]. Apart from these direct constructions of MOCSs, there are some other indirect methods to construct MOCSs such as interleaving, concatenation, paraunitary (PU) matrices, Kronecker product, extended correlation, etc. [?, ?, ?, ?, ?, ?]. However, the generated MOCSs may not be friendly for hardware generation due to their large space and time requirements. So how to construct MOCSs with flexible lengths is still an open problem.

Since the set size is constrained by the number of sub-carrier in MOCSs, which prevents the communication system from supporting a large number of users, Fan et $al.$ proposed the concept of ZCCSs in [?]. The reason why ZCCSs have large set sizes is that there is a zero correlation zone (ZCZ) in the aperiodic cross-correlation and auto-correlation. For an (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 M, N, L, Z refer to the set size, number of sub-carrier, length and ZCZ width, respectively. Especially, an (M, N, L, Z)-ZCCS is called an MOCS if $Z = L$. In the literature, ZCCSs are constructed by using direct and indirect methods. In [?], Wu et $al.$ proposed ZCCSs with length 2^m $(m > 0)$ based on GBFs, then they expanded the parameters of ZCCSs in 2021 [?]. Several GBFs based constructions of ZCCSs are

presented in the literature [?, ?, ?, ?]. Additionally, Tian et al. constructed ZCCS/OCS using RU matrices in [?]. Yi et al. applied Kronecker product to obtain ZCCS/GCS in [?]. Das et al. presented a class of ZCCSs by using Butson-type Hadamard (BH) matrices and optimal Z-paraunitary (ZPU) matrices [?]. Adhikary and Majhi in [?] employed Hadamard product to construct ZCCSs with new parameters. Further constructions of ZCCSs have been proposed in [?, ?, ?, ?]. In most previous designs, however, the optimal ZCCSs based on direct methods have limited lengths and the optimal ZCCSs based on indirect methods have limited hardware generations. Recently, Shen *et al.* introduced the concept of EBF and obtained optimal ZCCSs of length q^m [?], where $q \geq 2$ is a positive integer. This work helps us to construct more optimal ZCCSs.

Motivated by the existing works on MOCSs and ZCCSs, in this paper, we construct $(q^{d'}, q^{v+d}, \gamma)$-MOCSs with flexible lengths and $(q^{v+d}, q^d, q^m, q^{m-v})$-ZCCSs by using EBFs, where $\gamma = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u$, $0 < d' < d < m$, $v < m$, $a_k \in \mathbb{Z}_q$, $a_m \in \mathbb{Z}_q^*$ and $q \geq 2$ is a positive integer. According to the arbitrariness of q, the proposed MOCSs cover the result in [?] and have non-power-of-two lengths when $q = 2$. In addition, the resulting MOCSs and ZCCSs can be obtained directly from EBFs without using tedious sequence operations. Note that the proposed ZCSCSs are optimal with respect to the theoretical upper bound.

The remainder of this paper is outlined as follows. In Section 2, we give the notations and definitions that will be used throughout this paper. In Section 3, we show a construction of MOCS with flexible lengths. In Section 4, we present an construction optimal ZCCS. In Section 5, we make a comparison of the existing literature with this paper. Finally, we conclude this paper in Section 6.

2 Preliminaries

2.1 Notation

- $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ is the ring of integers modulo q, where $q \geq 2$ is a 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;

- $\lceil x \rceil$ denotes the smallest integer bigger than or equal to x;

3

- 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 (ACCF) $R_{\mathbf{a},\mathbf{b}}(\tau)$ between $\mathbf{a}$ and $\mathbf{b}$ at a time shift τ is defined as

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

If $\mathbf{a} = \mathbf{b}$, then $R_{\mathbf{a},\mathbf{b}}(\tau)$ is called the aperiodic auto-correlation function (AACF), denoted as $R_{\mathbf{a}}(\tau)$. In addition, by the definition of AACF, 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 $0 < |\tau| \leq L-1$,*

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

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 $0 \leq i \neq j \leq M-1$ and $0 \leq |\tau| \leq L-1$,*

$$R_{\mathcal{S}_i, \mathcal{S}_j}(\tau) = \sum_{k=0}^{N-1} R_{\mathbf{a}_k^i, \mathbf{a}_k^j}(\tau) = 0,$$

where each $\mathcal{S}_t = \{\mathbf{a}_0^t, \mathbf{a}_1^t, \cdots, \mathbf{a}_{N-1}^t\}$ 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*

$$R_{\mathcal{S}_i, \mathcal{S}_j}(\tau) = \sum_{k=0}^{N-1} R_{\mathbf{a}_k^i, \mathbf{a}_k^j}(\tau) = \begin{cases} NL, & \tau = 0, \ i = j, \\ 0, & 0 < |\tau| < Z, \ i = j, \\ 0, & |\tau| < Z, \ i \neq j, \end{cases}$$

where Z denotes the ZCZ width and each $\mathcal{S}_t = \{\mathbf{a}_0^t, \mathbf{a}_1^t, \cdots, \mathbf{a}_{N-1}^t\}$ consists of N length-L sequences for any $0 \leq t \leq M-1$. In addition, if $Z = L$, then the (M, N, L, Z)-ZCCS is called an (M, N, L)-MOCS.

The following results give two bounds on the parameters of MOCSs and ZCCSs, respectively.

Lemma 2.4. *[?] For an (M, N, L)-MOCS, the upper bound on set size satisfies the inequality $M \leq N$. When $M = N$, it is called a CCC.*

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

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

Note that a ZCCS is optimal if the above upper bound is achieved,i.e., $M = N \lfloor \frac{L}{Z} \rfloor$.

2.3 Extended Boolean functions (EBFs)

An EBF 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 $f = x_1 x_2 + x_1 + 2$ 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 $L \neq q^m$. Hence we define the corresponding truncated sequence $\mathbf{f}^{(L)}$ of the EBF f by removing the last $q^m - L$ elements of the sequence $\mathbf{f}$. That is $\mathbf{f}^{(L)} = (f_0, f_1, \cdots, f_{L-1})$ 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 [?]. For convenience, we ignore the superscript of $\mathbf{f}^{(L)}$ unless the sequence length is undetermined.

3 Construction of MOCSs with flexible lengths

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

Lemma 3.1. *[?] 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 $\mathbb{N}_m$ 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 $\mathbb{N}_v = \{\pi(1), \pi(2), \cdots, \pi(v)\}$.*

(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 $2 \leq t \leq m - k$.*

Let

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

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

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

5

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

Lemma 3.2. *For positive integers $m \geq 2$ and $r < m$, let h be a bijection from $S_1 = \mathbb{N}_r$ onto $S_2 \subseteq \mathbb{N}_m$ with r elements. Suppose that $h(u)$ is the smallest element of S_2. Let i be an integer with*

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

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

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

Proof. For convenience, we let $j = i - \sum_{\substack{l=1 \\ l \neq u}}^{r} a_l q^{h(l)-1}$ 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 $j^{(t)} = i^{(t)} - \sum_{\substack{l=1 \\ l \neq u}}^{r} a_l q^{h(l)-1}$ 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 $j^{(t)}$ in only one position k. 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,

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

$\square$

Lemma 3.3. *For positive integers $m \geq 2$ and $r < m$, let i and h be the same as that of Lemma ??. If $i \leq \sum_{\substack{l=1 \\ l \neq u}}^{r} a_l q^{h(l)-1} + q^{h(u)} - 1$ 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 $i_t = b \neq 0$ where $h(u) + 1 \leq t \leq m - 1$ and $t \neq h(l)$ for $l \in S_1 \setminus \{u\}$. Then we have $i \geq \sum_{\substack{l=1 \\ l \neq u}}^{r} a_l q^{h(l)-1} + b q^{t-1} \geq \sum_{\substack{l=1 \\ l \neq u}}^{r} a_l q^{h(l)-1} + q^{h(u)}$ which contradicts the condition. $\square$

Lemma 3.4. *[?] Let q be an even number, $(i_1, i_2, \cdots, i_m)$ and $(j_1, j_2, \cdots, j_m)$ be the binary representations of i and j, respectively, and let $\{I_1, I_2, \cdots, I_d\}$ be a partition of the set $\mathbb{N}_m$. Let π_α be a bijection from $\mathbb{N}_{m_\alpha}$ to I_α, where $|I_\alpha| = m_\alpha$ for any $\alpha \in \mathbb{N}_d$. If the following three conditions are satisfied:*

(1) α_1 is the largest integer satisfying $i_{\pi_\alpha(\beta)} = j_{\pi_\alpha(\beta)}$ for $\alpha \in \mathbb{N}_{\alpha_1}$ and $\beta \in \mathbb{N}_{m_\alpha}$.

(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 $j'_{\pi_{\alpha_1}(\beta_1 - 1)} = 1 - j_{\pi_{\alpha_1}(\beta_1 - 1)}$.
Then

$$f_{n,i} - f_{n,j} - f_{n,i'} + f_{n,j'} \equiv \frac{q}{2} \pmod{q},$$

where $f(x)$ as shown in Eq. (1) of [?].

Lemma 3.5. *Let $\boldsymbol{x}_{n_1}, \boldsymbol{x}_{n_2}, \cdots, \boldsymbol{x}_{n_d}$ be the sequences corresponding to EBFs $x_{n_1}, x_{n_2}, \cdots, x_{n_d}$, respectively, where $n_1 < n_2 < \cdots < n_d$. Let $\boldsymbol{u} = (u_0, u_1, \cdots, u_{L-1}) = a_1 \boldsymbol{x}_{n_1} \oplus a_2 \boldsymbol{x}_{n_2} \oplus \cdots \oplus a_d \boldsymbol{x}_{n_d}$ be a q-ary sequence with $a_i \in \mathbb{Z}_q$ for any $i \in \mathbb{N}_d$, which is a linear combination of $\boldsymbol{x}_{n_1}, \boldsymbol{x}_{n_2}, \cdots, \boldsymbol{x}_{n_d}$. If $q^{n_1} \mid L$ and $a_1 \neq 0$ let $(i_1, i_2, \cdots, i_m)$ be the binary representation of i and let $i^{(t)}$ differ from i in only one position n_1, i.e.,*

$$(i_1^{(t)}, i_2^{(t)}, \cdots, i_m^{(t)}) = (i_1, i_2, \cdots, i_{n_1-1}, i_{n_1} \oplus t, i_{n_1+1}, \cdots, i_m),$$

where $t \in \mathbb{Z}_q^*$. Then

$$\xi^{u_i} + \xi^{u_i(1)} + \xi^{u_i(2)} + \cdots + \xi^{u_i(q-1)} = 0.$$

Proof. Since $q^{n_1} \mid L$, then for any integer i,

$$u_{i(t)} - u_i = (a_1 i_{n_1}^{(t)} \oplus a_2 i_{n_2}^{(t)} \oplus \cdots a_k i_{n_k}^{(t)}) - (a_1 i_{n_1} \oplus a_2 i_{n_2} \oplus \cdots a_k i_{n_k}) \equiv a_1(i_{n_1}^{(t)} - i_{n_1}) \equiv a_1 t \pmod{q},$$

Thus we have

$$1 + \xi^{u_i(1) - u_i} + \xi^{u_i(2) - u_i} + \cdots + \xi^{u_i(q-1) - u_i} = 0.$$

$\square$

Now we state our construction in the following Theorem **??**, which is based on Lemma **??**.

Theorem 3.6. *Let m, d, d', v be positive integers with $0 < d' < d < m$ and $v < m$. Let $\{I_1, I_2, \cdots, I_d\}$ be a partition of the set $\mathbb{N}_{m-v}$. Put π_α be a bijection from $\mathbb{N}_{m_\alpha}$ to I_α, where*

$|I_\alpha| = m_\alpha$ for any $\alpha \in \mathbb{N}_d$. Let u be an integer with $\sum_{\alpha=1}^{d'} m_\alpha < u < \sum_{\alpha=1}^{d'+1} m_\alpha$, we impose an additional condition below:

$$\{\pi_1(1), \pi_1(2), \cdots, \pi_1(m_1), \pi_2(1), \cdots, \pi_{d'+1}(u')\} = \{1, 2, \cdots, u\},$$

where $0 < u' < m_{d'+1}$. 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

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

$$f_n^p(x) = f(x) + \sum_{\alpha=1}^{d} n_\alpha x_{\pi_\alpha(1)} + \sum_{k=1}^{v} n_{k+d} x_{m-v+k} + c \sum_{\alpha=1}^{d'} p_\alpha x_{\pi_\alpha(m_\alpha)}, \tag{2}$$

where $a_{\alpha,\beta}, c \in \mathbb{Z}_q^*$ are co-prime with q and $b_{\alpha,\beta,k}, c_{s,l}, c_0 \in \mathbb{Z}_q$. Then $\{\mathcal{F}^0, \mathcal{F}^1, \cdots, \mathcal{F}^{q^{d'}-1}\}$ generates a $(q^{d'}, q^{v+d}, L)$-MOCS with $L = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u$, $a_k \in \mathbb{Z}_q$ and $a_m \in \mathbb{Z}_q^*$, where $\mathcal{F}^p = \{\mathbf{f}_0^p, \mathbf{f}_1^p, \cdots, \mathbf{f}_{q^{v+d}-1}^p\}$.

Proof. Since for sequences $\mathbf{f}_n^p$ and $\mathbf{f}_n^{p'}$, $R_{\mathbf{f}_n^{p'}, \mathbf{f}_n^p}(-\tau) = R_{\mathbf{f}_n^p, \mathbf{f}_n^{p'}}^*(\tau)$, then it suffice to prove that for $0 \le p, p' \le q^{d'} - 1$ and $0 < \tau \le L - 1$,

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

where $f_{n,i}^p$ and $f_{n,j}^{p'}$ are the $(i+1)$-th and the $(j+1)$-th element of sequence $\mathbf{f}_n^p$ and $\mathbf{f}_n^{p'}$, respectively. For simplicity, we assume $a_k \ne 0$ for any $k \in \mathbb{N}_{v-1}$. 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. Let $(p_1, p_2, \cdots, p_{d'})$ and $(p_1', p_2', \cdots, p_{d'}')$ are the q-ary representations of p and p', respectively.

Case 1: If $i_{\pi_\alpha(1)} \ne j_{\pi_\alpha(1)}$ for some $\alpha \in \mathbb{N}_d$ or $i_{m-v+k} \ne j_{m-v+k}$ for some $k \in \mathbb{N}_v$. Then

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

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

Case 2: If $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ for all $\alpha \in \mathbb{N}_d$, $i_{m-v+k} = j_{m-v+k}$ for all $k \in \mathbb{N}_v$, and $i_m = j_m = 0$. Then

$$R_{\mathcal{F}^p, \mathcal{F}^{p'}}(\tau) = q^{d+v} \sum_{i=0}^{L-1-\tau} \xi^{f_i - f_j} \prod_{\alpha=1}^{d'} \xi^{p_\alpha i_{\pi_\alpha(m_\alpha)} - p_\alpha' j_{\pi_\alpha(m_\alpha)}}.$$

Similar to Lemma ??, we assume that

(1) α_1 is the largest integer satisfying $i_{\pi_\alpha(\beta)} = j_{\pi_\alpha(\beta)}$ for $\alpha \in \mathbb{N}_{\alpha_1}$ and $\beta \in \mathbb{N}_{m_\alpha}$.

(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, only in 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

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

and

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

which implies

$$R_{\mathcal{F}^{p_1}, \mathcal{F}^{p_2}}(\tau) = q^{d+v} \sum_{i=0}^{L-1-\tau} \xi^{f_i - f_j} \prod_{\alpha=1}^{d'} \xi^{p_\alpha i_{\pi_\alpha(m_\alpha)} - p'_\alpha j_{\pi_\alpha(m_\alpha)}} = 0.$$

Case 3: If $i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}$ for all $\alpha \in \mathbb{N}_d$, $i_{m-v+k} = j_{m-v+k}$ for all $k \in \mathbb{N}_v$, 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 $k < v$, i.e., $i_{m-v+k} = j_{m-v+k} = a_k \neq 0$ for $k \in \{k_1+1, k_1+2, \cdots, v\}$, then

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

$$\leq a_m q^{m-1} + \sum_{k=k_1+1}^{v-1} a_k q^{m-v+k-1} + q^{m-v+k_1-1} - 1.$$

According to Lemma ?? and $\pi_{\alpha_1(\beta_1-1)} < m - v + k_1 - 1$, 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 $\alpha \in \mathbb{N}_d$, $i_{m-v+k} = j_{m-v+k}$ for all $k \in \mathbb{N}_v$, 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 $k \in \mathbb{N}_v$,

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

According to Lemma **??**, we have $i_s = j_s = 0$ for $s = u + 1, u + 2, \cdots, m - v - 1$, so $\pi_{\alpha_1}(\beta_1) \leq u$, and $\pi_{\alpha_1}(\beta_1 - 1) \leq u$. 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 $R_{\mathcal{F}^p, \mathcal{F}^{p'}}(\tau) = 0$ for $0 < \tau \leq L - 1$.

Next, it remains to show that for $0 \leq p \neq p' \leq q^{d'} - 1$,

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

Since $p \neq p'$, there exists a smallest $s \in \mathbb{N}_{d'}$ such that $p_s \neq p'_s$. Then according to Lemma **??**, for any $0 \leq i \leq L - 1$, there exists $i^{(t)}$ whose q-ary representation differs from i in only one position s, i.e., $(i_1, i_2, \cdots, i_{s-1}, i_s \oplus t, i_{s+1}, \cdots, i_m)$ for any $t \in \mathbb{Z}_q^*$. Therefore, we get

$$\xi^{f_{n,i}^p - f_{n,i}^{p'}} + \xi^{f_{n,i(1)}^p - f_{n,i(1)}^{p'}} + \cdots + \xi^{f_{n,i(q-1)}^p - f_{n,i(q-1)}^{p'}}$$

$$= \xi^{f_{n,i}^p - f_{n,i}^{p'}} \left(1 + \xi^{f_{n,i(1)}^p - f_{n,i(1)}^{p'} - f_{n,i}^p + f_{n,i}^{p'}} + \cdots + \xi^{f_{n,i(q-1)}^p - f_{n,i(q-1)}^{p'} - f_{n,i}^p + f_{n,i}^{p'}} \right)$$

$$= \xi^{f_{n,i}^p - f_{n,i}^{p'}} \left(1 + \xi^{c(p_s - p'_s)} + \cdots + \xi^{c(p_s - p'_s)(q-1)} \right)$$

$$= 0$$

and

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

By the above discussion, we obtain that $\{\mathcal{F}^p \mid p \in \{0, 1, \cdots, q^{d'} - 1\}\}$ is a $(q^{d'}, q^{v+d}, L)$-MOCS with $L = a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u$, where $a_k \in \mathbb{Z}_q$ and $a_m \in \mathbb{Z}_q^*$.

$\square$

Remark 3.7. *In Theorem **??**, 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 coveblack in [?].*

Example 3.8. *Let $m = 5$, $v = 1$, $d = 2$, $d' = 1$, $m_1 = m_2 = 2$, $(\pi_1(1), \pi_1(2), \pi_2(1), \pi_2(2)) = (1, 2, 3, 4)$ and all $a_{\alpha,\beta}, b_{\alpha,\beta,k}, c_{s,l}, c_0, c$ are equal to 1. Then $\{\mathcal{F}^0, \mathcal{F}^1, \mathcal{F}^2\}$ forms a ternary $(3, 27, 108)$-MOCS from Theorem **??**.*

4 Constructions of CCCs and optimal ZCCSs

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

Theorem 4.1. *Let m, d be positive integers with $2 \leq d < m$, and $\{I_1, I_2, \cdots, I_d\}$ be a partition of the set $\mathbb{N}_m$. Put π_α be a bijection from $\mathbb{N}_{m_\alpha}$ to I_α, where $|I_\alpha| = m_\alpha$ for any $\alpha \in \{1, 2, \cdots, d\}$. Let*

$$f(x) = \sum_{\alpha=1}^{d} \sum_{\beta=1}^{m_\alpha-1} a_{\alpha,\beta} x_{\pi_\alpha(\beta)} x_{\pi_\alpha(\beta+1)} + \sum_{l=1}^{q-1} \sum_{u=1}^{m} h_{u,l} x_u^l + h_0,$$

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

where $a_{\alpha,\beta} \in \mathbb{Z}_q^*$ is 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 $\{\mathcal{F}^0, \mathcal{F}^1, \cdots, \mathcal{F}^{q^d-1}\}$ forms a q-ary CCC with $\mathcal{F}^p = \{\mathbf{f}_0^p, \mathbf{f}_1^p, \cdots, \mathbf{f}_{q^d-1}^p\}$.

Proof. The proof consists of two parts. In the first part, we demonstrate that for any $0 \leq p, p' \leq q^d - 1$ and $0 < \tau \leq q^m - 1$, $\mathcal{F}^p$ and $\mathcal{F}^{p'}$ satisfy the ideal correlation property, i.e.,

$$R_{\mathcal{F}^p, \mathcal{F}^{p'}}(\tau) = \sum_{n=0}^{q^d-1} R_{\mathbf{f}_n^p, \mathbf{f}_n^{p'}}(\tau) = \sum_{n=0}^{q^d-1} \sum_{i=0}^{q^m-1-\tau} \xi^{f_{n,i}^p - f_{n,j}^{p'}} = \sum_{i=0}^{q^m-1-\tau} \sum_{n=0}^{q^d-1} \xi^{f_{n,i}^p - f_{n,j}^{p'}} = 0,$$

where $f_{n,i}^p$ and $f_{n,j}^{p'}$ are the $(i+1)$-th and the $(j+1)$-th element of sequence $\mathbf{f}_n^p$ and $\mathbf{f}_n^{p'}$, respectively. Similarly, let the definitions of $i, j, i^{(t)}$ and $j^{(t)}$ be given as Theorem **??**. 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 $S_2(\tau) = \{i \mid \forall\, \alpha \in \{1, 2, \cdots, d\},\ 0 \leq$

$i \le q^m - 1 - \tau, \ i_{\pi_\alpha(1)} = j_{\pi_\alpha(1)}\}$. Thus we obtain that

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

where $(p_{k,1}, p_{k,2}, \cdots, p_{k,d})$ is the q-ary representation of p_k for any $k \in \{1, 2\}$. For any $i \in S_2(\tau)$, according to the Case 2 of first part in Theorem **??**, we have

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

and

$$
(\xi^{f_i - f_j} + \xi^{f_{i^{(1)}} - f_{j^{(1)}}} + \xi^{f_{i^{(2)}} - f_{j^{(2)}}} + \cdots + \xi^{f_{i^{(q-1)}} - f_{j^{(q-1)}}}) \prod_{\alpha=1}^{d} \xi^{p_\alpha i_{\pi_\alpha(m_\alpha)} - p'_\alpha j_{\pi_\alpha(m_\alpha)}} = 0.
$$

According to the above discussion, we know that the ideal correlation property is available for any $\tau > 0$. Now, we need to prove that for any $0 \le p \ne p' \le q^d - 1$ and $\tau = 0$,

$$
R_{\mathcal{F}^p, \mathcal{F}^{p'}}(0) = \sum_{n=0}^{q^d-1} R_{\mathbf{f}_n^p, \mathbf{f}_n^{p'}}(0) = \sum_{n=0}^{q^d-1} \sum_{i=0}^{q^m-1} \xi^{\sum_{\alpha=1}^{d} (p_\alpha \oplus p'_\alpha) i_{\pi_\alpha(m_\alpha)}} = 0.
$$

Put $\mathbf{d} = \sum_{\alpha=1}^{d} (p_\alpha \oplus p'_\alpha) \mathbf{x}_{\pi_\alpha(m_\alpha)}$. Due to each $\mathbf{x}_{\pi_\alpha(m_\alpha)}$ is a balanced sequence, the linear combination 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

$$
R_{\mathcal{F}^p, \mathcal{F}^{p'}}(0) = \sum_{n=0}^{q^d-1} \sum_{i=0}^{q^m-1} \xi^{\sum_{\alpha=1}^{d} (p_\alpha \oplus p'_\alpha) i_{\pi_\alpha(m_\alpha)}} = 0,
$$

which completes the proof.

$\square$

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

Theorem 4.2. *Let m, d, v be positive integers with $v \leq d$ and $v < m$, and let $\{I_1, I_2, \cdots, I_d\}$ a partition of the set $\mathbb{N}_m$, permutation π_α from $\mathbb{N}_{m_\alpha}$ into I_α, where $|I_\alpha| = m_\alpha$. Also for any $\alpha \in \mathbb{N}_d$. Also let*

$$f(x) = \sum_{\alpha=1}^{d} \sum_{\beta=1}^{m_\alpha - 1} a_{\alpha,\beta} x_{\pi_\alpha(\beta)} x_{\pi_\alpha(\beta+1)} + \sum_{l=1}^{q-1} \sum_{u=1}^{m} h_{u,l} x_u^l + h_0,$$

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

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 $\left\{ \mathcal{F}^0, \mathcal{F}^1, \cdots, \mathcal{F}^{q^{v+d}-1} \right\}$ forms a $(q^{v+d}, q^d, q^m, q^{m-v})$-ZCCS with $\mathcal{F}^p = \left\{ \mathbf{f}_0^p, \mathbf{f}_1^p, \cdots, \mathbf{f}_{q^d-1}^p \right\}$.

Proof. It is obvious that every sequence $\mathbf{f}_n^p$ can be divided into q^v relevant sub-sequence by a concatenate method, i.e.,

$$\mathbf{f}_n^p = \mathbf{g}_{n,0}^p | \mathbf{g}_{n,1}^p | \cdots | \mathbf{g}_{n,q^v-1}^p,$$

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

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

By the way of Theorem **??**, we conclude that the sequence set $\left\{ \mathbf{g}_{0,0}^p, \mathbf{g}_{1,0}^p, \cdots, \mathbf{g}_{q^d-1,0}^p \right\}$ forms a GCS. Therefore, we know that $\left\{ \mathbf{f}_0^p, \mathbf{f}_1^p, \cdots, \mathbf{f}_{q^d-1}^p \right\}$ satisfies the auto-correlation property for $0 < \tau \leq q^{m-v} - 1$.

Next, we verify the cross-correlation property, i.e., for $0 \leq p \neq p' \leq q^{v+d} - 1$ and for

any $0 < \tau < q^{m-v}$,

$$R_{\mathcal{F}^p,\mathcal{F}^{p'}}(\tau)$$

$$= \sum_{n=0}^{q^d-1} R_{\mathbf{f}_n^p,\mathbf{f}_n^{p'}}(\tau)$$

$$= \left(1 + \sum_{k=1}^{q^v-1} \xi^{u_k - w_k}\right) \sum_{n=0}^{q^d-1} R_{\mathbf{g}_{n,0}^p,\mathbf{g}_{n,0}^{p'}}(\tau) + \left(\xi^{-w_1} + \sum_{k=1}^{q^v-2} \xi^{u_k - w_{k+1}}\right) \sum_{n=0}^{q^d-1} R^*_{\mathbf{g}_{n,0}^{p'},\mathbf{g}_{n,0}^p}(q^v - \tau)$$

$$= 0,$$

where $\mathbf{f}_n^p = \mathbf{g}_{n,0}^p|(\mathbf{g}_{n,0}^p \oplus u_1)| \cdots |(\mathbf{g}_{n,0}^p \oplus u_{q^v-1})$ and $\mathbf{f}_n^{p'} = \mathbf{g}_{n,0}^{p'}|(\mathbf{g}_{n,0}^{p'} \oplus w_1)| \cdots |(\mathbf{g}_{n,0}^{p'} \oplus w_{q^v-1})$ with $u_i, w_i \in \mathbb{Z}_q$. The q-ary representations of p and p' are $(p_1, p_2, \cdots, p_{v+d})$ and $(p_1', p_2', \cdots, p_{v+d}')$, 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 $\mathbb{N}_{m-v}$. Obviously, according to Theorem **??**, we get that

$$\sum_{n=0}^{q^d-1} R_{\mathbf{g}_{n,0}^p,\mathbf{g}_{n,0}^{p'}}(\tau) = 0$$

and

$$\sum_{n=0}^{q^d-1} R^*_{\mathbf{g}_{n,0}^{p'},\mathbf{g}_{n,0}^p}(q^v - \tau) = 0.$$

This shows that $R_{\mathcal{F}^p,\mathcal{F}^{p'}}(\tau) = 0$. Similarly, we can prove that $R_{\mathcal{F}^p,\mathcal{F}^{p'}}(\tau) = 0$ for any $-q^d + 1 \le \tau < 0$.

When $\tau = 0$, for any $0 \le p \ne p' \le q^{v+d} - 1$,

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

The equality holds because $p \ne p'$ leads to the existence of at least one index $s \in \mathbb{N}_{v+d}$ such that $p_s \ne p_s'$ and $gcd(b,q) = 1$. By the above two cases, we get that $R_{\mathbf{f}^p,\mathbf{f}^{p'}}(\tau) = 0$ for any $-q^d < \tau < q^d$ and $0 \le p \ne p' \le q^{v+d}$. Thus we prove that $\left\{\mathcal{F}^0, \mathcal{F}^1, \cdots, \mathcal{F}^{q^{v+d}-1}\right\}$ is a $(q^{v+d}, q^d, q^m, q^{m-v})$-ZCCS with $\mathcal{F}^p = \left\{\mathbf{f}_0^p, \mathbf{f}_1^p, \cdots, \mathbf{f}_{q^d-1}^p\right\}$.

$\square$

Remark 4.3. *According to Lemma ??, we know the ZCCS constructed from Theorem ?? is optimal since $M/N = q^{v+d}/q^d = L/Z$ is available. In particular, when $v = 0$, the Theorem ?? changes into Theorem ??.*

Example 4.4. *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 ??. Then $\{\mathcal{F}^0, \mathcal{F}^1, \cdots, \mathcal{F}^{15}\}$ forms a quaternary $(16, 4, 64, 16)$-ZCCS, where $\mathcal{F}^3$ and $\mathcal{F}^{10}$ are given by*

$$
\begin{bmatrix} \mathbf{f}_0^3 \\ \mathbf{f}_1^3 \\ \mathbf{f}_2^3 \\ \mathbf{f}_3^3 \end{bmatrix} = \begin{bmatrix} 1212133132323311121213313232331112121331323233111212133132323311 \\ 1212200210102200121220021010220012122002101022001212200210102200 \\ 1212311332321133121231133232113312123113323211331212311332321133 \\ 1212022010100022121202201010002212120220101000221212022010100022 \end{bmatrix}
$$

$$
\begin{bmatrix} \mathbf{f}_0^{10} \\ \mathbf{f}_1^{10} \\ \mathbf{f}_2^{10} \\ \mathbf{f}_3^{10} \end{bmatrix} = \begin{bmatrix} 1133121231133232331130301331101011331212311332323311303013311010 \\ 1133232313312121331101013113030311332323133121213311010131130303 \\ 1133303031131010331112121331323211333030311310103311121213313232 \\ 1133010113310303331123233113212111330101133103033311232331132121 \end{bmatrix}
$$

The sum of aperiodic auto-correlation of sequences $\mathcal{F}^3$ is presented in Figure ?? and the sum of aperiodic cross-correlation of sequences $\mathcal{F}^3$ and $\mathcal{F}^{10}$ is presented in Figure ??.
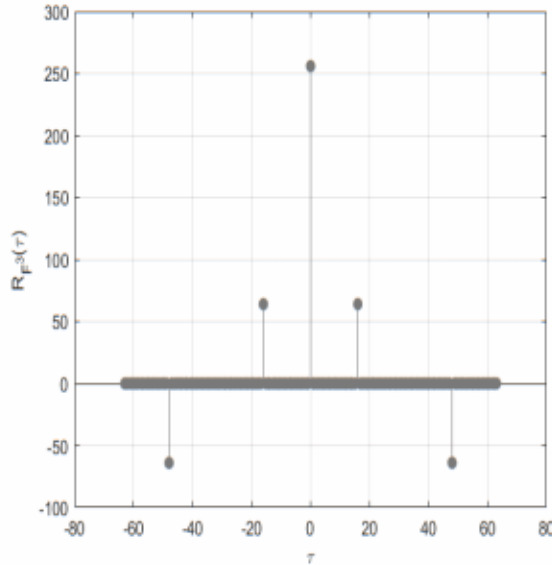

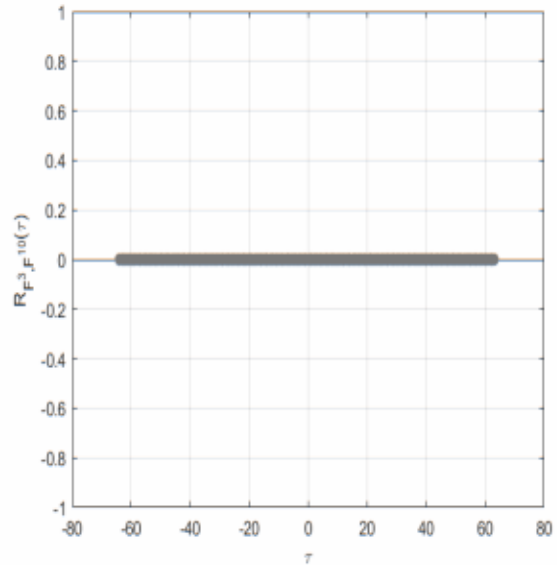Figure 1: Auto-correlation of $\mathcal{F}^3$ Figure 2: Cross-correlation of F^3 and $\mathcal{F}^{10}$

Table 1: Summary of Existing MOCSs

Source	Based on	Parameters	Conditions
[?]	GBF	$(2^k, 2^k, 2^m)$	$0 < k \le m$
[?]	GBF	$(2^{k'}, 2^{k+1}, 2^m + 2^t)$	$0 < k, t \le m; 0 \le k' \le t; k' \le k-1$
[?]	GBF	$(2^k, 2^{k+1}, 2^m + 2^t)$	$0 < k \le t \le m$
[?]	GBF	$(2^k, 2^{k+1}, 2^m + 2^t)$	$0 \le t < k \le m$
[?]	GBF	$(2^{k+1}, 2^{k+1}, 2^{m-1} + 2^{m-3})$	$k \le m-5$
[?]	q-ary function	(p^{n+1}, p^{n+1}, p^m)	p is a prime number, $0 < n < m$
[?]	MVF	$(\prod_{i=1}^k p_i^{n_i}, \prod_{i=1}^k p_i^{n_i}, \prod_{i=1}^k p_i^{m_i})$	$p_i	q$, q is a finite positive integer, $i \in \mathbb{N}_k, 0 < n_i \le m_i$
[?]	PU matrix	(M, M, M^m)	$m > 0$, M is the order of PU matrix
[?]	PU matrix	(M, M, N^m)	$N	M, m > 0$, M is the order of PU matrix
[?]	Kronecker product	$(M_1 M_2, M_1 M_2, N_1 N_2)$	(M_1, M_1, N_1)-CCC and (M_2, M_2, N_2)-CCC, $M1, M2, N_1, N_2$ are four even numbers
[?]	Kronecker product	$(M, M, MN_1 N_2)$	(M, M, N_1)-CCC and (M, M, N_2)-CCC, $2 \le M, N_1, N_2$
[?]	Extended correlation	$(MP, MP, 2N-1)$	(M, M, N)-CCC and (P, P, N)- CCC, $2 \le M, P, N$
[?]	concatenation	$(M_1 M_2/2, M_1 M_2/2, 2L_1 L_2)$	M_1, M_2 are two even numbers, L_1, L_2 are two positive integers
Theorem ??	EBF	$(q^{d'}, q^{v+d}, a_m q^{m-1} + \sum_{k=1}^{v-1} a_k q^{m-v+k-1} + q^u)$	$0 < d' < d < m$, $a_k \in \mathbb{Z}_q$, $a_m \in \mathbb{Z}_q^*$, and $q \ge 2$ is a positive integer

5 Comparison

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

From Table 1, we know that all GBFs-based MOCSs have lengths of 2^m or $2^m + 2^t$ [?, ?, ?, ?]. The constructions in [?] and [?] generate MOCSs with flexible lengths by using q-ary functions and MVFs, respectively. But both of these methods only have power of two lengths when $q = 2$. Other methods for designing MOCSs include PU matrices [?, ?], Interleavings, Kronecker product [?, ?], extended correlation [?] and concatenation [?]. However, these methods are hard to be applied in engineering due to their large space and time requirements in hardware generation. Compablack with the previous constructions, our results have flexible lengths as flexible non-power-of-two lengths when $q = 2$.

From Table 2, we know the constructions of ZCCSs in the literature mainly divided into direct and indirect approaches. The direct methods are mainly based on GBFs [?,?,?,?,?,?], Pseudo-Boolean functions (PBFs) [?,?], EBFs [?] and MVFs [?]. In fact, all existing ZCCSs constructed based on GBFs and PBFs have multiples of two lengths and the ZCCSs based on MVFs have limited set sizes. For other indirect methods, some researchers provided ZCCSs by Hadamard product [?], Z-complementary pairs (ZCPs) [?], BH matrix and optimal Z-paraunitary (ZPU) matrices [?]. These constructs are difficult to implement on hardware. In the case of the same length and ZCZ width, compablack to [?], the proposed ZCCSs have larger set sizes or lengths. Moreover, our ZCCSs can accommodate more users on the basis of achieving the optimality.

Table 2: Summary of Existing ZCCSs

Source	Based on	Parameters	Conditions	Optimal	Remark
[?]	GBF	$(2^{k+1}, 2^{k+1}, 3\cdot 2^m, 2^{m+1})$	$0 < k \le m$	×	Direct
[?]	GBF	$(2^{k+2}, 2^{k+2}, 2^m\cdot L, 2^m\cdot L')$	$L' > \frac{L}{2}$	✓	Direct
[?]	GBF	$(2^{k+1}, 2^{k+1}, 3\times 2^m, 2^{m+1})$	$m>0, k>0$	✓	Direct
[?]	GBF	$(2^{k+v}, 2^k, 2^m, 2^{m-v})$	$v\le m, k\le m-v$	✓	Direct
[?]	GBF	$(2^n, 2^n, 2^{m-1}+2, 2^{m-2}+2^{\pi(m-3)}+1)$	π is a permutation of $\mathbb{N}_{m-2}, m\ge 3$	✓	Direct
[?]	GBF	$(2^{n+1}, 2^{n+1}, 2^{m-1}+2, 2^{m-2}+2^{\pi(m-3)+1})$	π is a permutation of $\mathbb{N}_{m-2}, v\le m, q\ge 2, m\ge 2$	✓	Direct
[?]	GBF	$(2^{n+p}, 2^n, 2^m, 2^{m-p})$	$p\le m$	✓	Direct
[?]	GBF	$(2^{k+p+1}, 2^{k+1}, 2^m, 2^{m-p})$	$k+p\le m$	✓	Direct
[?]	GBF	$(2^{k+1}, 2^{k+1}, 3(2^{m-1}+2^{m-3}), 2(2^{m-1}+2^{m-3}))$	$m\ge 5, k>0$	✓	Direct
[?]	GBF	$(R2^{k+1}, 2^{k+1}, R(2^{m-1}+2^{m-3}), 2^{m-1}+2^{m-3})$	$m\ge 5, k>0,$ and R is even	✓	Direct
[?]	BH Matrix	(MP, M, MP, M)	M, P are the order of BH matrix	✓	Indirect
[?]	Optimal ZPU Matrix	$(MP, M, M^{N+1}P, M^{N+1})$	M, P are the order of BH matrix, $N>0$	✓	Indirect
[?]	Hadamard product	$(2^{n+1}, 2^{n+1}, N, Z)$	$N\ge 3, N$ is odd, $\lfloor \frac{N}{Z}=1\rfloor$	✓	Direct
[?]	ZCP	$(2^m, 2^m, L, Z)$	$Z\ge \lceil \frac{L}{2}\rceil$	✓	Direct
[?]	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, $n, m>0$	×	Direct
[?]	PBF	$(p2^{k+1}, 2^{k+1}, p2^m, 2^m)$	p is a prime	✓	Direct
[?]	MVF	$(\prod_{i=1}^k p_i^2, \prod_{i=1}^k p_i, \prod_{i=1}^k p_i^{m_i}, \prod_{i=1}^k p_i^{m_i-1})$	p_i is a prime number, $m_i>0$	✓	Direct
[?]	EBF	$(q^{v+1}, q, q^m, q^{m-v})$	$q\ge 2, v\le m$	✓	Direct
Theorem ??	EBF	$(q^{v+d}, q^d, q^m, q^{m-v})$	$v<m, d\le m-v, q\ge 2$ is a positive integer	✓	Direct

6 Conclusion

In this paper, we mainly present a construction of optimal ZCCSs and a construction of MOCSs with flexible lengths based on EBFs. According to the arbitrariness of q, the proposed MOCSs cover the result in [?] and have non-power-of-two lengths when $q = 2$. Moreover, the resulting MOCSs can be obtained directly from EBFs without using tedious sequence operations. The proposed MOCSs with flexible lengths find many applications in wireless communication due to its good correlation properties. The proposed ZCCSs are optimal with respect to the theoretical upper bound and we can obtain a new class of ZCCSs of arbitrary lengths with large zero correlation zone width.

Declarations

Conflicts of Interest The authors declare that they have no conflicts 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 (1961).

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

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

[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] 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).

[6] 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).

[7] 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).

[8] 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).

[9] Davis J. A., and Jedwab J.: Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Müller codes. IEEE Trans. Inf. Theory. **45**(7), 2397-2417 (1999).

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

[11] Li Y., and Chu W. B.: More Golay sequences. IEEE Trans. Inf. Theory. **51**(3), 1141-1145 (2005).

[12] Chen C. Y., Wang C. H., and Chao C. C.: Complementary sets and Reed-Müller codes for peak-to-average power ratio blackuction in OFDM. in Proc. 16th Int. Symp. AAECC. **3857**, 317-327 (2006).

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

[14] 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).

[15] 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).

[16] 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).

[17] Sarkar P., Li C., Majhi S., and Liu Z.: New correlation bound and construction of quasi-complementary code sets. arXiv: 2204.13538 (2022)

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

[19] 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).

[20] 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).

[21] 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).

[22] 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).

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

[24] Liu K., Liu J., and Ni J.: Generalized construction of Z-complementary code sets of odd length. IEEE Signal Process. Lett. **30**, 354-358 (2023).

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

[26] 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).

[27] Wu S. W., Sahin A., Huang Z. M., and Chen C. Y.: Z-complementary code sets with flexible lengths from generalized Boolean functions. IEEE Access. **9**, 4642-4652 (2021).

[28] 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).

[29] 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).

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

[31] Ghosh G., Majhi S., Paul S.: Construction of optimal binary Z-complementary code sets with new lengths. arXiv:2301.03294 (2023).

[32] Tian L., Li Y., Zhou Z., and Xu C.: Two classes of Z-complementary code sets with good cross-correlation subsets via paraunitary matrices. IEEE Trans. Commun. **69**(5), 2935-2947 (2021).

[33] Yu T., Adhikary A. R., Wang Y., and Yang Y.: New class of optimal Z-complementary code sets. IEEE Signal Process. Lett. **29**(5), 1477-1481 (2022).

[34] 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).

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

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

[37] 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. IEEE Signal Process. Lett. **29**, 872-876 (2022).

[38] 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).

[39] Roy A., Majhi S.: Construction of inter-group complementary code set and 2-D Z-complementary array code set based on multivariable functions. arXiv:2109.00970 (2021).

[40] Shen, B., Meng, H., Yang, Y. et al. New constructions of Z-complementary code sets and mutually orthogonal complementary sequence sets. Des. Codes Cryptogr. **91**, 353-371 (2023).

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

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

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

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