

# A Direct Construction of Complete Complementary Code with Zero Correlation Zone property for Prime-Power Length

Nishant Kumar, Sudhan Majhi, *Senior Member, IEEE*, and A.K. Upadhyay

## Abstract

In this paper, we propose a direct construction of a novel type of code set, which has combined properties of complete complementary code (CCC) and zero-correlation zone (ZCZ) sequences and called it complete complementary-ZCZ (CC-ZCZ) code set. The code set is constructed by using multivariable functions. The proposed construction also provides Golay-ZCZ codes with new lengths, i.e., prime-power lengths. The proposed Golay-ZCZ codes are optimal and asymptotically optimal for binary and non-binary cases, respectively, by *Tang-Fan-Matsufuzi* bound. Furthermore, the proposed direct construction provides novel ZCZ sequences of length  $p^k$ , where  $k$  is an integer  $\geq 2$ . We establish a relationship between the proposed CC-ZCZ code set and the first-order generalized Reed-Muller (GRM) code, and proved that both have the same Hamming distance. We also counted the number of CC-ZCZ code set in first-order GRM codes. The column sequence peak-to-mean envelope power ratio (PMEPR) of the proposed CC-ZCZ construction is derived and compared with existing works. The proposed construction is also deduced to Golay-ZCZ and ZCZ sequences which are compared to the existing work. The proposed construction generalizes many of the existing work.

## Index Terms

Golay complementary sets (GCSs), complete complementary code (CCC), multivariable functions, zero correlation zone (ZCZ) sequence set, Golay-ZCZ sequence set, CC-ZCZ code set, prime-power

length, peak-to-mean envelope power ratio (PMEPR), orthogonal frequency division multiplexing (OFDM), multi-carrier code division multiple access (MC-CDMA), generalized Reed-Muller (GRM) codes.

## I. INTRODUCTION

GOLAY was the first to introduce Golay complementary pair (GCP) in 1949 but defined formally in his article “Complementary Series” in 1960 [1]. GCPs show their applications in many areas such as infrared multislit spectrometry, orthogonal frequency-division multiplexing (OFDM) and many others. The idea of GCP was further extended to Golay complementary sets (GCSs) [2]. A relationship between GCP of length in the form  $2^m$  and generalized Boolean function (GBF) has been established in [3]. Later in [4], Paterson *et al.* obtained GCSs of polyphase sequences from cosets of the first-order generalized Reed-Muller (GRM) code. Further, an upper bound on peak-to-mean envelope power ratio (PMEPR) for second-order cosets of this code was obtained. In [5], the idea of GCSs was further extended to complete complementary codes (CCCs) which is a collection of GCSs with some extra aperiodic cross-correlation property. Additionally, CCC has found application in multi-carrier code division multiple access (MC-CDMA) systems to eliminate multiple-access interference (MAI) for multiple users over asynchronous environment [6], [7]. CCCs are also utilized in optimal channel estimation for multiple-input multiple-output (MIMO) frequency-selective fading channels [8], MIMO radar [9], [10], cell search in OFDM systems [11], and data hiding [12]. A detailed study on GCSs and CCCs can be carried out in [3], [4], [13]–[19].

In OFDM systems, GCSs are widely used to control PMEPR [3], an upper bound on PMEPR was obtained in [4]. By using the good aperiodic correlation properties of GCP and GCSs, these can be used for asynchronous CDMA system, channel estimation [20], synchronization [21], signal detection etc. Quasi-synchronous CDMA (QS-CDMA) system is proposed to reduce the impact of synchronization accuracy in communication systems [22]. QS-CDMA system can eliminate co-channel interference for multiuser environment when synchronization error is

controlled within a specific range [22].

Zero correlation zone (ZCZ) sequences have ideal periodic correlation property inside a zone about the origin. Therefore, they can reduce MAI and multipath interference (MPI) [23], and hence they are used to take benefit of quasi synchronization in the QS-CDMA system. They are also used in radar [24], channel estimation [25]–[27], pilot design [28], [29], multicode MIMO system [30], and as a training sequence in MIMO-OFDM systems [28]. The ZCZ sequences can achieve optimal channel estimation performance under the condition that all the received signals are quasi-synchronous within the ZCZ [31], [32].

The relation between GCSs and ZCZ sequences was first established in [33]. Later, numerous ZCZ sequences are constructed by using mutually orthogonal GCSs (MOGCS) [34]–[36]. While most of the ZCZ sequence constructions need predefined sequences like perfect sequences and use unitary matrices [36], interleaving technique [37] and Hadamard matrices [38]. The direct constructions of ZCZ sequences based on GBFs are provided in [39]–[41]. The connection between GRM codes and ZCZ sequences is also provided in [40], [41]. The GCSs and ZCZ sets are characterized by their aperiodic auto-correlation and periodic correlation properties, respectively. The authors in [42], [43], investigated the periodic auto-correlation behaviour of individual Golay sequences in 2013. Specifically, they presented two constructions of Golay sequences of length  $2^m$  each displaying a periodic zero auto-correlation zone (ZACZ) of  $2^{m-2}$ , and  $2^{m-3}$ , respectively, around the in-phase position. Motivated by the work in [42], [43], the authors in [44] studied the periodic zero cross-correlation zone (ZCCZ) of the GCSs presented in [18] and provided a relation between ZCZ sets and GCSs and proposed a construction of a new class of sequence sets and named it Golay-ZCZ sequence sets. Golay-ZCZ sequence set consists of sequences having their aperiodic auto-correlation sum zero except at the zero shift and ideal periodic cross-correlations and auto-correlations within the ZCZ. Precisely, a Golay-ZCZ sequence set is a ZCZ sequence set which is also a GCS. Therefore, from the application point of view, Golay-ZCZ sequence sets are used to obtain both the advantages in a single code.

For an instant, ZCZ sequences are used as pilots or training sequences in OFDM systems [28], [29] but it is not utilized for PMEPR reduction. Since Golay-ZCZ sequence sets are themselves GCSs, they can be utilized as training sequences as well as for PMEPR reduction. Therefore, the proposed code provides low PMEPR when employed in OFDM systems due to the good auto-correlation properties of GCSs. Besides, the Golay-ZCZ sets possess zero auto-correlations and cross-correlations within their ZCZ and hence have the potential application to synchronization. Inspired by the Golay-ZCZ work given in [44], the authors in [22] given construction of Golay-ZCZ sequence sets which have large ZCZ width. The length of proposed Golay-ZCZ sequence sets in [22] and [44] is limited to power-of-two. Continuing in this chain, recently in 2021, the authors in [45] provided a construction of Golay-ZCZ sequences of length  $M^2N$  using an CCC of length  $N$  and flock size  $M$ . Furthermore, in [46], they also constructed Golay-ZCZ complementary pair of length  $4N$ , where  $N$  is a positive integer and provided an open problem to construct Golay-ZCZ sequence set of non-power-of-two length as “*An interesting future work will be to design Golay-ZCZ sequence sets, consisting sequences of length non-power-of-two, which have periodic ZACZ\* and ZCCZ† around the in-phase position*”. Furthermore, they also extended this work to two-dimension [47].

Motivated by the above works, and open problem provided in [46], in this paper, we provide a construction of novel type of code set called CC-ZCZ code set of prime-power length in which each code is Golay-ZCZ sequence set having non-power-of-two length sequences which settles the open problem provided by in [46]. The proposed  $p$ -ary Golay-ZCZ sequence sets are asymptotically optimal with respect to *Tang-Fan-Matsufuji* bound and optimal for binary case. The proposed CC-ZCZ code sets are also seen as second-order cosets of first-order GRM codes. Since first-order GRM codes enjoy high Hamming distance, we prove that the proposed Golay-ZCZ sequence set in CC-ZCZ code set has the same Hamming distance as GRM codes.

\* zero auto-correlation zone    † zero cross-correlation zone

Additionally, we also count the number of cosets of GRM codes, which is further used to count the total number of CC-ZCZ code sets and Golay-ZCZ sequence sets. The column sequence PMEPR of the proposed CC-ZCZ construction is reduced. The row and column sequence PMEPR for Golay-ZCZ and CCC are also been reduced over the existing work [44] and [14], respectively. The proposed construction can generate new ZCZ sequences of length  $p^k$ , where  $k$  is a positive integer  $\geq 2$ . The proposed construction also contributes Golay-ZCZ sequence sets and ZCZ sequences which are again compared to the existing state-of-the-art.

The remainder of the paper is structured as follows. We provide some basic notations and definitions in Section II. In Section III, we provide the construction of CC-ZCZ code sets and provide examples in support of our construction. In Section IV, a relation between proposed CC-ZCZ code set and GRM codes is established. Moreover, the number of CC-ZCZ code set in a second-order coset of GRM code and Hamming distance are provided. In Section V, we discuss column sequence PMEPR of constructed CC-ZCZ code based MC-CDMA system. Section VI provides another result that increases the number of CC-ZCZ code sets. In section VII, we defend the work's novelty by comparing it to existing works in the literature. Lastly, we provide conclusion in Section VIII.

## II. PRELIMINARY

### A. Definition and Correlation Functions

Let  $\mathbf{a} = (a_0, a_1, \dots, a_{L-1})$  and  $\mathbf{b} = (b_0, b_1, \dots, b_{L-1})$  be two  $L$ -length complex-valued sequences. For an integer  $\tau$ , define

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

The function  $\mathcal{A}(\mathbf{a}, \mathbf{b})$  is referred to as aperiodic cross-correlation function (ACCF) of  $\mathbf{a}$  and  $\mathbf{b}$ . If  $\mathbf{a} = \mathbf{b}$  then this function is called aperiodic auto-correlation function (AACF) and denoted as  $\mathcal{A}(\mathbf{a})$ .

Further, the periodic cross-correlation function (PCCF) of  $\mathbf{a}$  and  $\mathbf{b}$  is defined as

$$\mathcal{P}(\mathbf{a}, \mathbf{b})(\tau) = \begin{cases} \sum_{i=0}^{L-1} a_i b_{(i+\tau) \bmod L}^*, & 0 \leq \tau < L, \\ \sum_{i=0}^{L-1} a_i b_{(i-\tau) \bmod L}^*, & -L < \tau < 0. \end{cases} \quad (2)$$

When  $\mathbf{a} = \mathbf{b}$ , then this function is called periodic auto-correlation function (PACF) and denoted as  $\mathcal{P}(\mathbf{a})$  [48].

*Definition 1:* Let  $\mathbf{C} = \{\mathbf{C}_0, \mathbf{C}_1, \dots, \mathbf{C}_{K-1}\}$  be a collection of  $K$  matrices (codes) of order  $M \times L$ . Define

$$\mathbf{C}_\xi = \begin{bmatrix} \mathbf{a}_0^\xi \\ \mathbf{a}_1^\xi \\ \vdots \\ \mathbf{a}_{M-1}^\xi \end{bmatrix}, \quad (3)$$

where  $\mathbf{a}_v^\xi$  ( $0 \leq v \leq M-1, 0 \leq \xi \leq K-1$ ) is the  $v$ th row sequence or  $v$ th constituent sequence.

Then the ACCF of two codes  $\mathbf{C}_{\xi_1}, \mathbf{C}_{\xi_2} \in \mathbf{C}$  is defined as

$$\gamma(\mathbf{C}_{\xi_1}, \mathbf{C}_{\xi_2})(u) = \sum_{v=0}^{M-1} \gamma(\mathbf{a}_v^{\xi_1}, \mathbf{a}_v^{\xi_2})(u). \quad (4)$$

*Definition 2:* Let  $\mathbf{C}$  be a code set satisfying the following correlation properties

$$\gamma(\mathbf{C}_{\xi_1}, \mathbf{C}_{\xi_2})(u) = \begin{cases} LM, & \xi_1 = \xi_2 \text{ and } u = 0, \\ 0, & \xi_1 = \xi_2 \text{ and } 0 < |u| < L, \\ 0, & \xi_1 \neq \xi_2 \text{ and } |u| < L. \end{cases} \quad (5)$$

Then  $\mathbf{C}$  is known as  $(K, M, L)$ -MOGCS. If  $K = M$ , it is referred to be CCC set and we write it as  $(K, K, L)$ -CCC. Additionally, each code of  $\mathbf{C}$  is known as GCS [49]. When  $M = 2$  it is called GCP [19].

*Definition 3:* Let  $\mathcal{Z} = \{\mathbf{z}_0, \mathbf{z}_1, \dots, \mathbf{z}_{K-1}\}$  be a set of  $K$  sequences each of length  $L$ , i.e.,

$$\mathbf{z}_i = (\mathbf{z}_{i0}, \mathbf{z}_{i1}, \dots, \mathbf{z}_{iL-1}), \quad 0 \leq i \leq K-1.$$

Then,  $\mathcal{Z}$  is referred to be  $(K, L, Z)$ -ZCZ sequence set for  $0 \leq i, j \leq K - 1$ , if  $\mathcal{Z}$  satisfies the following,

$$\mathcal{P}(\mathbf{z}_i, \mathbf{z}_j)(u) = \begin{cases} 0, & i = j \text{ and } 1 \leq |u| < Z, \\ 0, & i \neq j \text{ and } 0 \leq |u| < Z, \\ L, & i = j \text{ and } u = 0, \end{cases} \quad (6)$$

where  $Z$  is termed as ZCZ width.

*Definition 4: (Tang-Fan-Matsufuji Bound [50])* Let  $\mathcal{Z}$  be any ZCZ sequence set with parameter  $(K, L, Z)$ . Then,  $KZ \leq L$  and if  $KZ = L$ , then  $\mathcal{Z}$  is said to be optimal. If for the larger value of  $K$ ,  $KZ \approx L$ ,  $\mathcal{Z}$  is said to be asymptotically optimal. For the binary case, it is widely accepted that the bound is reduced to  $2KZ \leq L$  [51].

*Definition 5:* Let  $\mathcal{Z}$  be a  $(K, L, Z)$ -ZCZ sequence set then  $\mathcal{Z}$  is called  $(K, L, Z)$ -Golay-ZCZ sequence set if it additionally satisfies the GCS properties.

*Definition 6:* Let  $\mathbf{C} = \{\mathbf{C}_0, \mathbf{C}_1, \dots, \mathbf{C}_{K-1}\}$  be a  $(K, K, L)$ -CCC. Then  $\mathbf{C}$  is called  $(K, K, L, Z)$ -CC-ZCZ code set if each  $\mathbf{C}_i$ ,  $\forall i = 0, 1, \dots, k - 1$  is  $(K, L, Z)$ -Golay-ZCZ sequence set.

## B. Multivariable Functions and Corresponding Sequences [14]

Let  $\mathbf{x} = (x_1, x_2, \dots, x_{k-1}) \in \mathbb{Z}_p^k$ , be a vector of finite length, where  $p$  is a prime number and  $k$  is a positive integer. It is clear that  $x_i \in \mathbb{Z}_p$  for  $1 \leq i \leq k$ . Now, we take a specific collection of monomials of degree at most  $r$  over the variables  $x_1, x_2, \dots, x_k$  as follows

$$\mathcal{M}(\mathbf{x}, r) = \{x_1^{j_1} x_2^{j_2} \dots x_k^{j_k} : j_i \in \{0, 1\} \text{ for } 1 \leq i \leq k, j_1 + j_2 + \dots + j_k \leq r\}, \quad (7)$$

where  $0 \leq r \leq k$ . A monomial's degree in  $\mathcal{M}$  is determined by the number of independent variables associated with it and this can be verified by examining the expressions of the monomials in  $\mathcal{M}$ . A linear combination of monomials in  $\mathcal{M}$  with  $\mathbb{Z}_q$ -valued coefficients, where  $q$  is a positive integer, leads to a multivariable function  $f(x_1, x_2, \dots, x_k) : \mathbb{Z}_p^k \rightarrow \mathbb{Z}_q$  which has maximum degree

$r$ . Let  $\mathcal{F}(\mathcal{M}(\mathbf{x}, r), q)$  be the set of all multivariable functions  $f(x_1, x_2, \dots, x_k) : \mathbb{Z}_p^k \rightarrow \mathbb{Z}_q$ , over the monomials in  $\mathcal{M}$  and defined as

$$\mathcal{F}(\mathcal{M}(\mathbf{x}, r), q) = \left\{ \sum_{(j_1, j_2, \dots, j_k) \in \{0,1\}^k} c_{j_1, j_2, \dots, j_k} x_1^{j_1} x_2^{j_2} \dots x_k^{j_k} : c_{j_1, j_2, \dots, j_k} \in \mathbb{Z}_q \right\}, \quad (8)$$

where  $r$  is the maximum degree of a multivariable function  $f$  in  $\mathcal{F}(\mathcal{M}(\mathbf{x}, r), q)$ . When  $p = 2$ , the set of multivariable functions  $\mathcal{F}(\mathcal{M}(\mathbf{x}, r), q)$  is reduced to a set of  $\mathbb{Z}_q$ -valued GBFs of maximum degree  $r$  over the vector variable  $\mathbf{x}$ .

For a multivariable function,  $f \in \mathcal{F}(\mathcal{M}(\mathbf{x}, r), q)$ , the  $\mathbb{Z}_q$ -valued sequence  $\theta(f)$  and the complex-valued sequence  $\Theta(f)$  having length  $p^k$  are defined as

$$\theta(f) = (f_0, f_1, \dots, f_{p^k-1}), \quad (9)$$

$$\Theta(f) = (\omega^{f_0}, \omega^{f_1}, \dots, \omega^{f_{p^k-1}}). \quad (10)$$

where  $f_i = f(i_0, i_1, \dots, i_{k-1})$ ,  $\omega = \exp(2\pi\sqrt{-1}/q)$ , and  $(i_0, i_1, \dots, i_{k-1})$  is the  $p$ -ary vector representation of  $i$ .

### C. Generalized Reed-Muller (GRM) Code

For a prime  $p$ , let  $\lambda = p^n$  and  $n \geq 1$ , then codewords of  $\lambda$ -ary GRM codes consist of the sequence corresponding to multivariable polynomials over the field  $\mathbb{F}_\lambda$ , where  $\lambda = p^n$  and  $n \geq 1$ . Let us consider a polynomial ring  $\mathbb{F}_\lambda[x_1, x_2, \dots, x_m]$  with  $m$  variables. The GRM code with parameters  $m$  and  $r$  consists of all the sequences corresponding to polynomials with  $m$  variables and degree no larger than  $r$ .

*Definition 7:* The  $r$ -th order  $r \leq \lambda$ ,  $\lambda$ -ary GRM code denoted by  $GRM_\lambda(m, r)$ , is defined by the set of  $\lambda$ -ary vectors as

$$GRM_\lambda(m, r) = \{\theta(f) : f \in \mathbb{F}_\lambda[x_1, x_2, \dots, x_m], \deg(f) \leq r\}. \quad (11)$$

It is to be noted that we always have  $x^\lambda = 1$  in  $\mathbb{F}_\lambda$ , so we only need to consider polynomials in which the degree of each  $x_i$  is no larger than  $\lambda - 1$ . All such polynomials with degree no larger

than  $r$  are linear combinations of the following set of monomials

$$\mathcal{N}(r) = \left\{ x_1^{j_1} x_2^{j_2}, \dots, x_m^{j_m} : j_i = 0, 1, 2, \dots, \lambda - 1 \text{ and } \sum_{i=1}^m j_i \leq r \right\}. \quad (12)$$

Using combinatorics, we can always prove that the number of monomials in the set  $\mathcal{N}(r)$  is,  $|\mathcal{N}(r)| = \sum_{d=0}^r \binom{m-1+d}{d}$ . It is well known that  $\mathbb{F}_\lambda[x_1, x_2, \dots, x_m]$  forms a vector space over the field  $\mathbb{F}_\lambda$ , further it can be easily proved that  $GRM_\lambda(m, r)$  is its subspace. Therefore,  $GRM_\lambda(m, r)$  is a linear code with code length  $n = \lambda^m$  and code dimension  $\sum_{d=0}^r \binom{m-1+d}{d}$ . Moreover, if we arrange sequences corresponding to monomials in  $\mathcal{N}(r)$  as the rows of a matrix then this matrix forms a generator matrix of  $GRM_\lambda(m, r)$ .

*Lemma 1 ( [52]):* For  $\lambda = p^n$  and  $n \geq 1$ , minimum Hamming distance of  $GRM_\lambda(m, r)$  is  $(R+1).p^Q$ , where  $R$  is the remainder and  $Q$  is the quotient resulting from dividing  $m(p-1) - r$  by  $p-1$ .

#### D. Peak-to-Mean Envelope Power Ratio (PMEPR)

In spite of several benefits arising from the OFDM technique, its wide acceptance has been hindered by its high PMEPR in uncoded signals. In this subsection, we define PMEPR for OFDM signals.

One can model the OFDM signal for a complex valued word  $\mathbf{B} = (B_1, B_2, \dots, B_N)$  of length  $N$  as the real part of the

$$\mathcal{S}_{\mathbf{B}}(\tau) = \sum_{i=1}^N B_i e^{2\pi(i+\zeta)(\tau)\sqrt{-1}}, \quad (13)$$

where  $0 \leq \tau < 1$  and  $\zeta$  is a positive constant. The sequence  $\mathbf{B} = (B_1, B_2, \dots, B_N)$  is termed as modulating codeword of the OFDM symbol. The PMEPR of word  $\mathbf{B}$  is defined as

$$PMEPR(\mathbf{B}) = \frac{1}{N} \sup_{0 \leq \tau < 1} |\mathcal{S}_{\mathbf{B}}(\tau)|^2. \quad (14)$$

It is to be observed that the largest value that PMEPR can have is  $N$ . However, it is preferable to use codewords with a lower PMEPR than  $N$ . Additionally, the PMEPR of GCS of size  $M$  is bounded above by  $M$  [4].

### III. PROPOSED CONSTRUCTION OF CC-ZCZ CODE SET

In this section, we provide a construction of CC-ZCZ code set of prime-power length. For that we start with a result which provides the construction of CCC of prime-power length [14]. For the ease of representation, we present this result in a modified way without losing the essence of the result.

*Lemma 2* ([14]): For an integer  $m \geq 2$ , let  $\{1, 2, \dots, m\}$  is divided into  $k$  partitions namely,  $E_1, E_2, \dots, E_k$  where  $1 \leq k \leq m - 1$ . Further, let us also assume that  $\lambda = p^n$  and  $n \geq 1$  and  $\pi_\beta$  be bijection mapping from  $\{1, 2, \dots, n_\beta\}$  to  $E_\beta$  where  $n_\beta = |E_\beta| \geq 1, \forall \beta = 2, 3, \dots, k$  and  $n_1 = |E_1| \geq 2$ . Now, we define a multivariable function  $f : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_\lambda$  as

$$f(x_1, x_2, \dots, x_m) = \frac{\lambda}{p} \sum_{\beta=1}^k \sum_{\gamma=1}^{n_\beta-1} x_{\pi_\beta(\gamma)} x_{\pi_\beta(\gamma+1)} + \sum_{\alpha=1}^m g_\alpha x_\alpha, \quad (15)$$

where  $g_\alpha \in \mathbb{Z}_\lambda$  for  $\alpha = 1, 2, \dots, m$ . Further, let  $\mathbf{u}_k = [u_1, u_2, \dots, u_k]$ ,  $\mathbf{v}_k = [v_1, v_2, \dots, v_k]$  be  $p$ -ary representation for  $0 \leq \mathbf{u}_k, \mathbf{v}_k \leq p^k - 1$ . Define

$$a_{\mathbf{u}_k}^{\mathbf{v}_k} = a_{u_1}^{v_1}(E_1) + a_{u_2}^{v_2}(E_2) + \dots + a_{u_k}^{v_k}(E_k), \quad (16)$$

where for any  $1 \leq \beta \leq k$ , multivariable function  $a_{u_\beta}^{v_\beta}(E_\beta)$  is defined as

$$a_{u_\beta}^{v_\beta}(E_\beta) = \frac{\lambda}{p} \sum_{\gamma=1}^{n_\beta-1} x_{\pi_\beta(\gamma)} x_{\pi_\beta(\gamma+1)} + \sum_{\gamma=1}^{n_\beta} g_{\pi_\beta(\gamma)} x_{\pi_\beta(\gamma)} + \frac{\lambda}{p} x_{\pi_\beta(1)} u_\beta + \frac{\lambda}{p} x_{\pi_\beta(n_\beta)} v_\beta. \quad (17)$$

Let us also define

$$\mathbf{C}_{\mathbf{u}_k} = [\Theta(a_{\mathbf{u}_k}^{\mathbf{v}_k})]_{0 \leq \mathbf{v}_k \leq p^k - 1} = \begin{bmatrix} \Theta(a_{\mathbf{u}_k}^0) \\ \Theta(a_{\mathbf{u}_k}^1) \\ \vdots \\ \Theta(a_{\mathbf{u}_k}^{p^k-1}) \end{bmatrix}. \quad (18)$$

Then  $\mathbf{C} = \{\mathbf{C}_{\mathbf{u}_k} : 0 \leq \mathbf{u}_k \leq p^k - 1\}$  is  $(p^k, p^k, p^m)$ -CCC.

*Theorem 1:* For a fixed  $\mathbf{u}_k$ ,  $\mathbf{C}_{\mathbf{u}_k}$  is GCS as defined in Lemma 2. Let  $\mathbf{C}'_{\mathbf{u}_k}$  be  $\mathbf{C}_{\mathbf{u}_k}$  together with the permutation  $\pi_\beta(1) = m - \beta + 1$  for  $\beta = 1, 2, \dots, k$ . Then  $\mathbf{C}'_{\mathbf{u}_k}$  is  $(p^k, p^m, (p-1)p^{\pi_1(2)-1})$ -Golay-ZCZ sequence set and hence  $\mathbf{C}' = \{\mathbf{C}'_{\mathbf{u}_k} : 0 \leq \mathbf{u}_k \leq p^k - 1\}$  is  $(p^k, p^k, p^m, (p-1)p^{\pi_1(2)-1})$ -CC-ZCZ code set.

*Proof:* Please see Appendix A. ■

*Remark 1:* If we have  $\pi_1(2) = m - k$ , then from *Theorem 1*,  $\mathbf{C}'_{\mathbf{u}_k}$ , is  $(p^k, p^m, (p-1)p^{m-k-1})$ -ZCZ  $\forall 0 \leq \mathbf{u}_k \leq p^k - 1$ , which implies  $KZ = (p-1)p^{m-1}$  and  $L = p^m$ . Now, for  $\lambda = 2$ ,  $KZ = 2L$  and hence  $\mathbf{C}'_{\mathbf{u}_k}$  is optimal ZCZ sequence set. But if  $p \neq 2$  then for larger value of  $p$ ,  $(p-1) \approx p$  and hence  $KZ \approx L$ , therefore, in this case,  $\mathbf{C}'_{\mathbf{u}_k}$  is asymptotically optimal.

According to *Theorem 1*, we can provide a construction of  $(p^k, p^k, p^m, (p-1)p^{\pi_1(2)-1})$ -CC-ZCZ code sets having variable ZCZ width  $\pi_1(2)$ . It is desirable to have a larger ZCZ width, we take  $\pi_1(2) = m - k$  to propose a family of  $(p^k, p^k, p^m, (p-1)p^{m-k-1})$ -CC-ZCZ code sets having larger ZCZ width. Furthermore, each code of CC-ZCZ is  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence set and it is optimal (*Tang-Fan-Matsufuji Bound*) for  $\lambda = 2$  and asymptotically optimal for  $\lambda \neq 2$ . To support our construction, we present examples below.

*Example 1: (Binary Case)* Taking  $\lambda = 2, p = 2, k = 2$ , and  $m = 5$ , we let  $E_1 = \{1, 3, 5\}$  and  $E_2 = \{2, 4\}$  be a partition of  $\{1, 2, 3, 4, 5\}$ . Also let  $\pi_1(1) = 5, \pi_1(2) = 3, \pi_1(3) = 1, \pi_2(1) = 4$  and  $\pi_2(2) = 2$ . Let  $f : \mathbb{Z}_2^5 \rightarrow \mathbb{Z}_2$  be defined as

$$f(x_1, x_2, \dots, x_5) = x_5x_3 + x_3x_1 + x_4x_2 + x_1 + x_3.$$

Further, let  $\mathbf{u}_k = 0$ , Then

$$\begin{aligned} \mathbf{C}'_0 &= \begin{bmatrix} \theta(a_0^0) \\ \theta(a_0^1) \\ \theta(a_0^2) \\ \theta(a_0^3) \end{bmatrix} = \begin{bmatrix} \theta(f + x_5 \cdot 0 + x_4 \cdot 0 + x_1 \cdot 0 + x_2 \cdot 0) \\ \theta(f + x_5 \cdot 0 + x_4 \cdot 0 + x_1 \cdot 1 + x_2 \cdot 0) \\ \theta(f + x_5 \cdot 0 + x_4 \cdot 0 + x_1 \cdot 0 + x_2 \cdot 1) \\ \theta(f + x_5 \cdot 0 + x_4 \cdot 0 + x_1 \cdot 1 + x_2 \cdot 1) \end{bmatrix} \\ &= \begin{bmatrix} 01011111011011000101000001100011 \\ 00001010001110010000010100110110 \\ 01101100010111110110001101010000 \\ 00111001000010100011011000000101 \end{bmatrix}, \end{aligned}$$

where the above matrix is phase matrix and  $C'_0$  is a  $(4, 32, 4)$ -Golay-ZCZ sequence set. Moreover, we can also derive  $C'_1, C'_2$  and  $C'_3$  and these are also  $(4, 32, 4)$ -Golay-ZCZ sequence sets. Hence  $C' = \{C'_0, C'_1, C'_2, C'_3\}$  is a  $(4, 4, 32, 4)$ -CC-ZCZ code set. Since  $K = 4, L = 32, Z = 4$  which implies  $KZ = 16$ . Hence,  $2KZ = L$ . Therefore,  $C'_i$  is optimal by *Tang-Fan-Matsufuji* Bound. A graphical representation of periodic correlation of sequences in  $C'_0$  is shown in Fig. 1

*Example 2: (Non-binary case)* Here let  $\lambda = 3, k = 2, m = 3$  and  $p = 3$ . Also let  $E_1 = \{2, 3\}, E_2 = \{1\}$  be a partition of  $\{1, 2, 3\}$ . Further, let  $\pi_1(1) = 3, \pi_1(2) = 2$ , and  $\pi_2(1) = 1$ . Define  $f : \mathbb{Z}_3^3 \rightarrow \mathbb{Z}_3$  as  $f(x_1, x_2, x_3) = x_3x_2$ . Now, let us fix  $\mathbf{u}_k = \mathbf{0}$  then

$$C'_0 = \begin{bmatrix} a_0^0 \\ a_0^1 \\ a_0^2 \\ a_0^3 \\ a_0^4 \\ a_0^5 \\ a_0^6 \\ a_0^7 \\ a_0^8 \end{bmatrix} = \begin{bmatrix} f + x_3.0 + x_1.0 + x_2.0 + x_1.0 \\ f + x_3.0 + x_1.0 + x_2.1 + x_1.0 \\ f + x_3.0 + x_1.0 + x_2.2 + x_1.0 \\ f + x_3.0 + x_1.0 + x_2.0 + x_1.1 \\ f + x_3.0 + x_1.0 + x_2.1 + x_1.1 \\ f + x_3.0 + x_1.0 + x_2.2 + x_1.1 \\ f + x_3.0 + x_1.0 + x_2.0 + x_1.2 \\ f + x_3.0 + x_1.0 + x_2.1 + x_1.2 \\ f + x_3.0 + x_1.0 + x_2.2 + x_1.2 \end{bmatrix} = \begin{bmatrix} 000000000012012012021021021 \\ 012012012021021021000000000 \\ 021021021000000000012012012 \\ 000111222012120201021102210 \\ 012120201021102210000111222 \\ 021102210000111222012120201 \\ 000222111012201120021210102 \\ 012201120021210102000222111 \\ 021210102000222111012201120 \end{bmatrix}, \quad (19)$$

$C'_0$  is a  $(9, 27, 2)$ -Golay-ZCZ sequence set. Similarly,  $C'_{\mathbf{u}_k}$  for  $1 \leq \mathbf{u}_k \leq 8$  are also  $(9, 27, 2)$ -Golay-ZCZ sequence set. Hence  $C' = \{C'_0, C'_1, \dots, C'_8\}$  is a  $(9, 9, 27, 2)$ -CC-ZCZ code set.

#### IV. CC-ZCZ CODE SETS FROM GRM CODES

In this section, a relation between CC-ZCZ code set and elements of second-order coset of  $GRM_p(m, 1)$  is established for  $\lambda = p$ . The precise number of cosets and number of CC-ZCZ code set in each coset is also given. Hamming distance of Golay-ZCZ sequence is also calculated.

It can be obtained that if we have a sequence in  $C'_{\mathbf{u}_k}$ , then it is a codeword belonging to

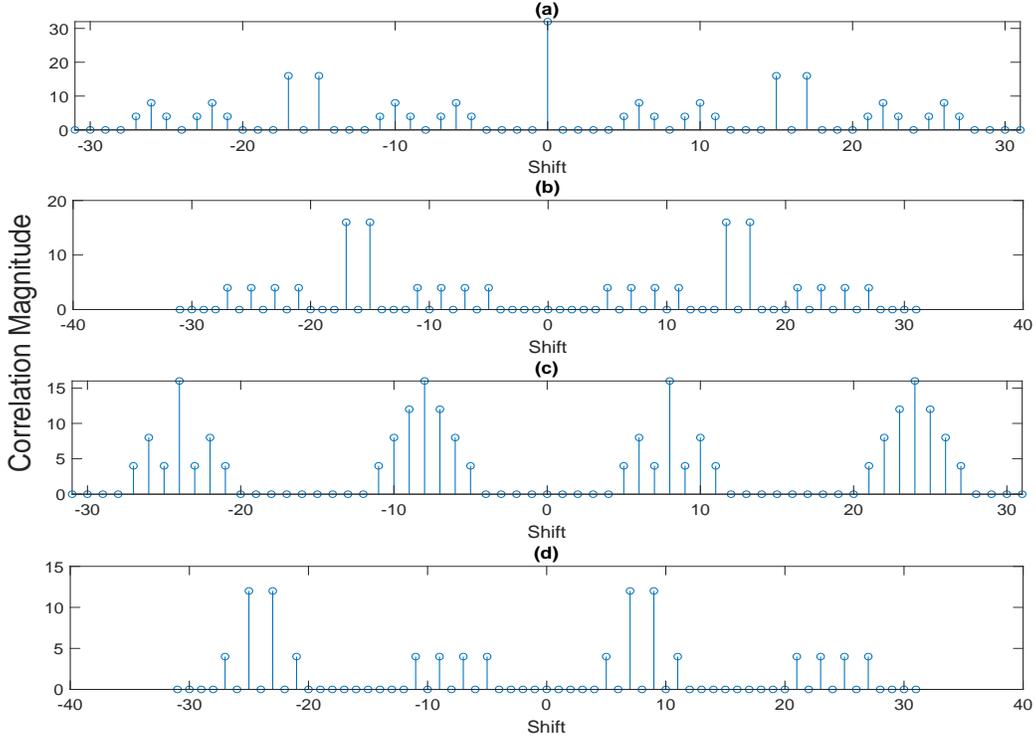


Fig. 1: (a) Auto-correlation plot for  $\{\theta(a_0^0), \theta(a_0^1), \theta(a_0^2), \theta(a_0^3)\}$ , (b) Cross-correlation plot for  $\{(\theta(a_0^1), \theta(a_0^2)), (\theta(a_0^3), \theta(a_0^4))\}$ , (c) Cross-correlation plot for  $\{(\theta(a_0^1), \theta(a_0^3)), (\theta(a_0^2), \theta(a_0^4))\}$  (d) Cross-correlation plot for  $\{(\theta(a_0^1), \theta(a_0^4)), (\theta(a_0^2), \theta(a_0^3))\}$ .

second-order coset  $\mathcal{Q}_1 + GRM_p(m, 1)$  where  $\mathcal{Q}_1$  is given by

$$\mathcal{Q}_1 = \sum_{\beta=1}^k \sum_{\gamma=1}^{n_\beta-1} x_{\pi_\beta(\gamma)} x_{\pi_\beta(\gamma+1)}. \quad (20)$$

Conversely, if any sequence is in the coset  $\mathcal{Q}_1 + GRM_p(m, 1)$  then it belongs to a certain  $(p^k, p^m, (p-1)p^{\pi_1(2)-1})$ -Golay-ZCZ sequence set. Now, let us consider the constructed  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence family by taking  $\pi_1(2) = m - k$ .

*Corollary 1:* The number of coset representative  $\mathcal{Q}_1$  in the second-order coset of the form  $\mathcal{Q}_1 + GRM_p(m, 1)$  is given by

$$\sum_{n_1+n_2+\dots+n_k=m} \binom{m-k-1}{n_1-2, n_2-1, \dots, n_k-1} (n_1-2)! \prod_{\beta=2}^k (n_\beta-1)!. \quad (21)$$

*Proof:* Since, we have  $\pi_1(1) = m$  and  $\pi_1(2) = m - k$ , so we can get  $(n_1 - 2)!$  different quadratic forms of the type

$$x_{\pi_1(1)}x_{\pi_1(2)} + x_{\pi_1(2)}x_{\pi_1(3)} + \cdots + x_{\pi_1(n_1-1)}x_{\pi_1(n_1)}, \quad (22)$$

where  $\pi_1(i)$  is a permutation of  $n_1 - 2$  integers where  $i = 3, 4, \dots, n_1$ . Similarly, there are  $(n_\beta - 1)!$  different quadratic forms of the type  $\sum_{\beta=1}^{n_\beta-1} x_{\pi_\beta(\gamma)}x_{\pi_\beta(\gamma+1)}$  for  $\beta = 2, 3, \dots, k$  as  $\pi_\beta(1)$  is restricted to  $m - \beta + 1$ . In addition, we have the condition  $n_1 + n_2 + \cdots + n_k = m$  where  $n_\beta = |E_\beta|$  and non-empty sets  $E_1, E_2, \dots, E_k$  form a partition of  $\{1, 2, \dots, m\}$ . Therefore, we can explicitly determine the number of distinct coset representatives  $\mathcal{Q}_1$  as

$$\sum_{n_1+n_2+\cdots+n_k=m} \binom{m-k-1}{n_1-2, n_2-1, \dots, n_k-1} (n_1-2)! \prod_{\beta=2}^k (n_\beta-1)!.$$

■

*Corollary 2:* Let  $\mathcal{Q}_1 + GRM_p(m, 1)$  be any second-order coset with coset representative  $\mathcal{Q}_1$  and let  $\pi_1(2) = m - k$ . Then the coset  $\mathcal{Q}_1 + GRM_p(m, 1)$  consists of  $p^{m-k+1}$  and  $p^{m+1}$  distinct  $p$ -ary  $(p^k, p^k, p^m, (p-1)p^{m-k-1})$ -CC-ZCZ code set and  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence set respectively.

*Proof:* We have from *Theorem 1*, that a codeword  $\mathbf{c}$  in  $\mathcal{Q}_1 + GRM_p(m, 1)$  lies in the  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence set

$$\mathbf{C}'_{\mathbf{u}_k} = \left\{ f + \sum_{\beta=0}^{k-1} x_{\pi_{\beta+1}(1)} u_{\beta+1} + \sum_{\beta=1}^k x_{\pi_\beta(n_\beta)} v_\beta + b_0 : v_\beta \in \mathbb{Z}_p, 1 \leq \beta \leq k \right\}. \quad (23)$$

So it can easily be obtained that for a fixed value of  $\mathbf{u}_k$ ,  $\mathcal{Q}_1 + GRM_p(m, 1)$  consists of  $p^{m-k+1}$  distinct  $p$ -ary  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence set. Hence, we have  $p^{m-k+1}$  distinct  $p$ -ary  $(p^k, p^k, p^m, (p-1)p^{m-k-1})$ -CC-ZCZ code set. Since  $\mathbf{u}_k$  can vary in  $p^k$  ways, therefore,  $\mathcal{Q}_1 + GRM_p(m, 1)$  consists of  $p^{m-k+1} \cdot p^k = p^{m+1}$  distinct  $p$ -ary  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence set.

■

Since the codes in our construction lie inside the second-order cosets of first-order  $GRM$  codes, therefore, they have the high Hamming distance. Hamming distance of a code measures how efficient a code is to detect and correct errors. If the Hamming distance of a code is  $h$  then we can correct the errors of Hamming weight less than  $h/2$ . Therefore, in the next corollary, we prove that minimum Hamming distance of the constructed CC-ZCZ code set is equal to minimum Hamming distance of  $GRM_p(m, 1)$ .

*Corollary 3:* The minimum Hamming distance of  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence sets which are constructed in *Theorem 1* is  $(p-1)p^{m-1}$ .

*Proof:* Since,  $C'_{\mathbf{u}_k}$  is contained in the second-order coset

$$\mathcal{Q}_1 + GRM_p(m, 1) = \{\mathcal{Q}_1 + c : c \in GRM_p(m, 1)\}. \quad (24)$$

Hence, according to *Lemma 1*,  $C'_{\mathbf{u}_k}$  has the minimum Hamming distance  $(p-1)p^{m-1}$ . ■

Considering  $p$ -ary sequences, let  $N(\mathcal{Q}_1)$  be the number of coset representatives  $\mathcal{Q}_1$ ,  $N(GZ)$  be the number of distinct  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence set in a coset  $\mathcal{Q}_1 + GRM_p(m, 1)$ ,  $N(CZ)$  be the number of distinct  $(p^k, p^k, p^m, (p-1)p^{m-k-1})$ -CC-ZCZ code set in a coset  $\mathcal{Q}_1 + GRM_p(m, 1)$ , and  $d(\mathcal{Q}_1 + GRM_p(m, 1))$  be the minimum Hamming distance of  $\mathcal{Q}_1 + GRM_p(m, 1)$ . Taking  $p = 3$  in *corollary 1*, *corollary 2*, and *corollary 3*, Table I shows the values of  $N(\mathcal{Q}_1)$ ,  $N(GZ)$ ,  $N(CZ)$  and  $d(\mathcal{Q}_1 + GRM_3(m, 1))$  for lengths 27, 81, and 243. Taking  $m = 5$  and  $k = 1$ , it can be observed from Table I that there are 6 second-order cosets  $\mathcal{Q}_1 + GRM_3(5, 1)$  and each coset consists of 243 distinct  $(3, 3, 243, 54)$ -CC-ZCZ code set. If we want to increase the set size from 3 to 9, we need to take  $k = 2$ . Then, Table I gives that we can obtain 81,  $(9, 9, 243, 18)$ -CC-ZCZ code set with reduced ZCZ width from one of 6 different second-order cosets  $\mathcal{Q}_1 + GRM_3(5, 2)$ .

## V. PMEPR OF PROPOSED CC-ZCZ CODE SET

In this section, a method has been discussed to reduce column sequence PMEPR of proposed CC-ZCZ code set. Since in the proposed CC-ZCZ code set, each code is Golay-ZCZ sequence set

TABLE I: Calculated Values of  $N(\mathcal{Q}_1)$ ,  $N(GZ)$ ,  $(K, L, Z)$  and  $d(\mathcal{Q}_1 + GRM_3(m, 1))$ .

m	k	(K, K, L, Z)	$N(\mathcal{Q}_1)$	$N(\mathbf{CZ})$	$N(\mathbf{GZ})$	$d(\mathcal{Q}_1 + \mathbf{GRM}_3(m, 1))$
3	1	(3, 3, 27, 6)	1	27	81	18
	2	(9, 9, 27, 2)	1	9		18
4	1	(3, 3, 81, 18)	2	81	243	54
	2	(9, 9, 81, 6)	2	27		54
	3	(27, 27, 81, 2)	1	9		54
5	1	(3, 3, 243, 54)	6	243	729	162
	2	(9, 9, 243, 18)	6	81		162
	3	(27, 27, 243, 6)	3	27		162
	4	(81, 81, 243, 2)	1	9		162

of size  $p^k$  and hence its row sequence PMEPR is bounded by  $p^k$ . But column sequence PMEPR of CC-ZCZ can further be reduced. If we want to generate  $j$ th column of  $\mathbf{C}'_{\mathbf{u}_k}$ ,  $0 \leq j \leq p^m - 1$  given in (23) then only variable terms in (23) is  $\sum_{\beta=1}^k x_{\pi_\beta(n_\beta)} v_\beta$ . Now, we add some constant to it and we can get,

$$\phi_j(v) = \frac{\lambda}{p} \sum_{\beta=1}^{k-1} v_{\pi'(\beta)} v_{\pi'(\beta+1)} + \frac{\lambda}{p} \sum_{\beta=1}^k j_{\pi_\beta(n_\beta)} v_\beta + \frac{\lambda}{p} v_{\pi'(1)} t + \frac{\lambda}{p} v_{\pi'(k)} l \quad (25)$$

where  $l, t, v \in \mathbb{Z}_p$ ,  $\pi'$  be the permutation of symbols  $1, 2, \dots, k$ ,  $[v_1, v_2, \dots, v_k]$  be the  $p$ -ary representation of  $v$ . By putting  $m = k$  and  $k = 1$  in Lemma 2 it can easily be seen that  $\Theta(\phi_j(v))$  is a member of a GCS which has  $p$  sequences each of length  $p^k$ . Hence its column sequence PMEPR is bounded by  $p$ . Now, let us redefine  $\mathbf{C}'_{\mathbf{u}_k}$  as

$$\mathbf{C}'_{\mathbf{u}_k} = \left\{ f + \frac{\lambda}{p} \sum_{\beta=0}^{k-1} x_{\pi_{\beta+1}(1)} u_{\beta+1} + \phi_x(v) + b_0 : v_\beta \in \mathbb{Z}_p, 1 \leq \beta \leq k \right\}, \quad (26)$$

where

$$\phi_x(v) = \frac{\lambda}{p} \sum_{\beta=1}^{k-1} v_{\pi'(\beta)} v_{\pi'(\beta+1)} + \sum_{\beta=1}^k x_{\pi_\beta(n_\beta)} v_\beta + \frac{\lambda}{p} v_{\pi'(1)} t + \frac{\lambda}{p} v_{\pi'(k)} l. \quad (27)$$

For some multivariable functions  $g_1, g_2$  and constants  $c_1, c_2$ , it can easily be verified that

$$\begin{aligned} \mathcal{A}(g_1 + c_1) &= \mathcal{A}(g_1), \\ \mathcal{A}(g_1 + c_1, g_2 + c_2) &= \mathcal{A}(g_1, g_2) \omega^{c_1 - c_2}, \\ \mathcal{P}(g_1 + c_1) &= \mathcal{P}(g_1), \\ \mathcal{P}(g_1 + c_1, g_2 + c_2) &= \mathcal{P}(g_1, g_2) \omega^{c_1 - c_2}. \end{aligned} \quad (28)$$

Using (28), we can assure that redefining of  $\mathbf{C}'_{\mathbf{u}_k}$  as in (26) affect its correlation properties by a multiplication of constant, i.e.,  $\mathbf{C}'_{\mathbf{u}_k}$  appearing in (26) is still a Golay-ZCZ sequence set whose column sequence PMEPR is bounded by  $p$ .

*Remark 2:* In [44], the PMEPR of Golay-ZCZ sequence set is upper bounded by the number of sub-carriers, i.e.,  $2^k$ . The PMEPR of Golay-ZCZ sequence set increases with the increase in the value of  $k$ . On the other hand, in the proposed Golay-ZCZ sequence set, the number of sub-carriers is  $p^k$  and upper bound for its column sequence PMEPR is  $p$ . For  $p = 2$ , we have  $2^k$  sub-carriers and maximum column sequence PMEPR 2, which remains same with increase in the value of  $k$ . So, the proposed construction have advantage over the construction presented in [44] as maximum column sequence PMEPR of the proposed construction is bounded above by 2 for  $2^k$  sub-carriers.

*Remark 3:* Although, we have taken CCCs from [14], but authors in [14] didn't bound the column sequence PMEPR in proposed construction. In the proposed construction, we bound the maximum column sequence PMEPR of CCCs having flock size  $p^k$  by  $p$ .

## VI. MORE CC-ZCZ CODE SETS

In this section, another construction of CC-ZCZ code set is provided which are different from those generated from *Theorem 1*. Similar to CC-ZCZ constructed in *Theorem 1*, we also provide number of cosets of GRM codes, number of CC-ZCZ code set in each coset, and Hamming distance but omit the proof as they are same as proof given in section IV.

*Theorem 2:* For a fixed  $\mathbf{u}_k$ ,  $C_{\mathbf{u}_k}$  is GCS as defined in *Lemma 2*. Let  $C''_{\mathbf{u}_k}$  be  $C_{\mathbf{u}_k}$  together with the permutation  $\pi_\beta(n_\beta) = m - k + \beta$ , for  $\beta = 1, 2, \dots, k$ . Then  $C''_{\mathbf{u}_k}$  is  $(p^k, p^m, (p-1)p^{\pi_k(n_k-1)-1})$ -Golay-ZCZ sequence set and hence  $C'' = \{C''_{\mathbf{u}_k} : 0 \leq \mathbf{u}_k \leq p^k - 1\}$  is  $(p^k, p^k, p^m, (p-1)p^{\pi_k(n_k-1)-1})$ -CC-ZCZ code set.

*Corollary 4:* The number of coset representative  $\mathcal{Q}_2$  in the second-order coset of the form  $\mathcal{Q}_2 + GRM_p(m, 1)$  is given by

$$\sum_{n_1+n_2+\dots+n_k=m} \binom{m-k-1}{n_1-1, n_2-1, \dots, n_k-2} (n_k-2)! \prod_{\beta=1}^{k-1} (n_\beta-1)!, \quad (29)$$

where

$$\mathcal{Q}_2 = \sum_{\beta=1}^k \sum_{\gamma=1}^{n_\beta-1} x_{\pi_\beta(\gamma)} x_{\pi_\beta(\gamma+1)}. \quad (30)$$

*Corollary 5:* Let  $\mathcal{Q}_2 + GRM_p(m, 1)$  be any second-order coset with coset representative  $\mathcal{Q}_2$  as defined in (30) and let  $\pi_k(n_k-1) = m - k$ . Then coset  $\mathcal{Q}_2 + GRM_p(m, 1)$  consists of  $p^{m-k+1}$  and  $p^{m+1}$  distinct  $p$ -ary  $(p^k, p^k, p^m, (p-1)p^{m-k-1})$ -CC-ZCZ code set and  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence set respectively.

*Corollary 6:* The minimum Hamming distance of  $(p^k, p^m, (p-1)p^{m-k-1})$ -Golay-ZCZ sequence sets which are constructed in *Theorem 2* is  $(p-1)p^{m-1}$ .

## VII. COMPARISON WITH EXISTING WORKS

Since the construction of CC-ZCZ is not available in the literature therefore in this section, the contributed Golay-ZCZ sequences, ZCZ sequences, and PMEPR of Golay-ZCZ sequences and CCCs are compared with existing works along with comparison tables.

### A. Comparison with existing constructions of Golay-ZCZ Sequence Set

1) *Comparison with [22], [44]:* In [44], authors proposed the construction of  $(2^k, 2^m, 2^{\pi_1(2)-1})$ -Golay-ZCZ sequence sets. In our construction (*Theorem 1*), if we take  $p = 2$  then the parameters of Golay-ZCZ sequence sets in [44] appear as special case of our parameters of Golay-ZCZ sequence sets. Similarly, in [22], parameters of proposed  $(2^k, 2^m, 2^{\pi_k(n_k)-1})$ -Golay-ZCZ sequence sets appear as special case of ours for  $p = 2$  in *Theorem 2*.

2) *Comparison with [45], [46]:* In [45], authors proposed an indirect construction of  $(M, (M-1)N, M^2N)$ -Golay-ZCZ sequence set with the help of  $(M, M, N)$ -CCC. This construction requires CCC as a seed code to construct Golay-ZCZ sequence set which makes it indirect. Furthermore, in the proposed construction, we are getting Golay-ZCZ sequence set through a multivariable function which makes our construction direct and advantageous over [45]. In [46], authors proposed an indirect construction of Golay-ZCZ complementary pair of length  $4N$  using GCPs of length  $N$ , having ZCZ width  $N + 1$ . This construction can produce only GCPs but not GCSs. Moreover, length of sequence is also dependent on length of GCP because the construction is indirect. On the other hand, the proposed construction is direct which is based on multivariable functions. Furthermore, the proposed construction can produce GCPs (for  $p = 2$ ) as well as GCSs (for  $p \neq 2$ ).

A detailed comparison of contributed Golay-ZCZ sequences with existing works is provided in Table II.

### B. Comparison with existing constructions of ZCZ Sequences

The constructions of ZCZ sequences based on RM codes or Boolean functions [39], [40], [44], multivariable functions [41], bent functions [53], and perfect non-linear function [54] are direct constructions of ZCZ sequences available in the literature while many constructions need kernel sequences such as perfect sequences [36]–[38], [55]. Although, constructions presented in [39], [40], [44] are direct but length of ZCZ sequences is limited to power-of-two only. In [53]

TABLE II: Comparison with [22], [44]–[46]

Author, Reference	Based on	Parameter (K,L,Z) & Constraints	Direct/Indirect	Optimality
Chen <i>et. al.</i> , [44]	GBF of order 2	$(2^k, 2^m, 2^{\pi_1(2)-1})$ , $\pi_\alpha(1) = m - \alpha + 1$ , $1 \leq \beta \leq k$	Direct	Optimal for binary case
Wang <i>et. al.</i> , [22]	GBF of order 2	$(2^k, 2^m, 2^{\pi_k(n_k-1)-1})$ , $\pi_\alpha(n_\alpha) = m - k + \alpha$ , $1 \leq \beta \leq k$	Direct	Optimal for binary case
Gu <i>et. al.</i> , [45]	$(M, M, N)$ -CCC	$(M, (M - 1)N, M^2N)$	Indirect	Optimal for binary case
Gu <i>et. al.</i> , [46]	Concatenation of GCP	$(2, 4N, N)$ , $N$ is a positive integer	Indirect	Asymptotically optimal
Theorem 1	Second-order multivariable functions	$(p^k, p^m, (p - 1)p^{\pi_1(2)-1})$ , $p$ is prime and $\pi_\beta(1) = m - \beta + 1$ , $1 \leq \beta \leq k$	Direct	Optimal for binary case else asymptotically optimal
Theorem 2	Second-order multivariable functions	$(p^k, p^m, (p - 1)p^{\pi_k(n_k-1)-1})$ , $p$ is prime and $\pi_\beta(n_\beta) = m - k + \beta$ , $1 \leq \beta \leq k$	Direct	Optimal for binary case else asymptotically optimal

and [54], the length of ZCZ sequences is limited to  $N^2$  and  $p^2$  respectively, where  $p$  is an odd prime, and  $N$  is a positive integer. Hence flexibility in length parameter is not adequate here. Furthermore, in [41], authors provided a direct construction of ZCZ sequences having flexible length, i.e.,  $p^n$ , where  $n$  is a positive integer  $\geq 3$  but it is unable to produce ZCZ sequences of length  $p^2$ . The proposed construction can generate ZCZ sequences of length  $p^n$ , where  $n$  is a positive integer  $\geq 2$ . A detailed comparison is provided in Table III.

### C. Comparison with PMEPR of Existing Works.

In this section, the proposed PMEPR of CC-ZCZ code set is compared with the PMEPR of existing constructions of CCCs, detailed comparison is provided in Table IV. It can be observed from the Table IV that if we put  $p = 2$  in our construction then, the parameter of CCCs presented in [13], [18], [56], [57] and Golay-ZCZ sequence sets presented in [22], [44] can be obtained from our construction. Furthermore, since PMEPR of our CC-ZCZ code set is bounded by 2 hence it has advantage over [13], [18], [22], [44], [57] and PMEPR of our CC-ZCZ code set coincide with PMEPR of CCC in [56]. Additionally, the authors in [14] presented a construction

TABLE III: Comparison with [35], [44], [55], [40], [54], [53], and [39]\*

Author, Reference	Based on	Parameter $(K, L, Z)$	Direct/Indirect	Optimality
Tang <i>et al.</i> , [35]	MOGCS	$(2^n, 2^{n+1}Z_{cz}, Z_{cz} + 1), n \geq 1$	Indirect	Optimal
Chen <i>et al.</i> , [44]	Generalised Boolean function	$(2^k, 2^m, 2^{m-k-1}), m \geq 2, \text{ and } k \leq m - 1.$	Direct	Optimal for binary case
Hayashi <i>et al.</i> , [55]	Perfect sequences	$(2(2n + 1), 4(2k + 1)(2n + 1), 4k + 1), n \geq 1, k \geq 1$	Indirect	Neither optimal nor almost optimal
Liu <i>et al.</i> , [40]	Second-order Reed-Muller codes	$(2^{k+1}, 2^{n+k+2}, 2^n), k \geq 0, n \geq 1$	Direct	Optimal for binary case
Zhou <i>et al.</i> , [54]	Perfect non-linear function	$(p, p^2, p), p \text{ is an odd prime}$	Direct	Optimal
Zhang <i>et al.</i> , [53]	Generalised Bent function	$(N, N^2, N), N \text{ is positive integer.}$	Direct	Optimal.
Tang <i>et al.</i> , [39]	Generalised Boolean function	$(2^k, 2^m, 2^{m-k} - 2^{m-k-z}), k \geq 0, n \geq 1$	Direct	optimal if $m = k + z$ and almost optimal if $m = k + z + 1$
Kumar <i>et al.</i> , [41]	Multivariable functions	$(p^t, p^{n+t+1}, (p-1)p^n), n, t \geq 1, p \text{ is prime and } t \leq n$	Direct	Optimal for binary case else asymptotically optimal
Theorem 1 and Theorem 2	Multivariable functions	$(p^k, p^m, (p-1)p^{m-k-1}), p \text{ is prime}$	Direct	Optimal for binary case else asymptotically optimal

\* The parameters presented in table are according to the definition of ZCZ in the corresponding paper. However, changing the definition of ZCZ also changes the bound and hence it doesn't affect the optimality of ZCZ sequence sets.

of CCCs but did not bound the column sequence PMEPR. In Section V, we tackled this problem and provided a bound for column sequence PMEPR of CCC.

## VIII. CONCLUSION

In this paper, we settled open problem provided by Gong. *et al.* by providing a direct construction of  $(p^k, p^k, p^m, (p-1)p^{\pi_1(2)-1})$ -CC-ZCZ code set and  $(p^k, p^m, (p-1)p^{\pi_1(2)-1})$ -Golay-ZCZ sequence set using multivariable functions. The proposed construction provides the non-power-of-two sequence length and larger ZCZ width. We are interested in larger ZCZ width therefore by substituting  $\pi_1(2) = m - k$ ,  $(p^k, p^m, (p-1)p^{m-k-1})$ -CC-ZCZ code set is achieved, in which each Golay-ZCZ sequence set is asymptotically optimal for non-binary case else optimal, with respect to *Tang-Fan-Matsufuji* Bound. We also established a relation between proposed CC-ZCZ code set and GRM codes and provided minimum Hamming distance of such codes. Moreover, the proposed construction provides tighter upper bound for column sequence PMEPR of proposed CC-ZCZ code set. The comparison of the proposed construction in the context of

TABLE IV: Comparison of the PMEPR of construction with [13], [18], [22], [44]–[46], [56], [57]

Author, Ref.	Parameters	Based on	Constraints	Column sequence PMEPR is upper bounded by
Rathinakumar <i>et. al.</i> , [13]	$(2^{k+1}, 2^{k+1}, 2^m)$ -CCC	GBF of order 2	$m, k \in \mathbb{Z}^+, m > 1$	$2^{k+1}$
Chen <i>et. al.</i> , [18]	$(2^k, 2^k, 2^m)$ -CCC	GBF of order $> 2$	$k, m \in \mathbb{Z}^+, m \geq 1, k \leq m$	$2^k$
Wang <i>et. al.</i> [22]	$(2^k, 2^m, 2^{m-k-1})$ -Golay-ZCZ	GBF	$m, k \in \mathbb{Z}^+, 1 \leq k \leq m - 1$	$2^k$
Chen <i>et. al.</i> [44]	$(2^k, 2^m, 2^{m-k-1})$ -Golay-ZCZ	GBF	$m, k \in \mathbb{Z}^+, 1 \leq k \leq m - 1$	$2^k$
Gu <i>et. al.</i> , [45]	$(M, (M - 1)N, M^2N)$ -Golay-ZCZ	CCC	There exist a $(M, M, N)$ -CCC	$M$
Gu <i>et. al.</i> [46]	$(2, 4N, N)$ -Golay-ZCZ	Concatenation of GCP	$N$ is a positive integer	2
Z. Liu, [56]	$(2^{k+1}, 2^{k+1}, 2^m)$ -CCC	GBF of order $> 2$	$m, k \in \mathbb{Z}^+, m > 1$	2
Wu <i>et. al.</i> , [57]	$(2^k, 2^k, 2^m)$ -CCC	GBF of order 2	$m, k \in \mathbb{Z}^+, m \geq 3, 1 \leq k \leq m$	$2^k$
This paper*	$(p^k, p^k, (p - 1)p^{m-k-1}, p^m)$ -CC-ZCZ	MVF of order 2	$k, m \in \mathbb{Z}^+, p$ is prime	$p$

\* In this paper CCCs are directly taken from [14] but we have bounded the column sequence PMEPR of these CCCs.

Golay-ZCZ sequences, ZCZ sequences, and PMEPR is provided. Further, relying on the existing literature, we propose two open problems as

- 1) *Construction of CC-ZCZ code set and Golay-ZCZ sequence set having length in the form of product of different primes.*
- 2) *Since each code in CC-ZCZ code set is ZCZ sequence set so we can treat CC-ZCZ code set as multiple ZCZ sequence set. Hence, it would be interesting to find inter-set ZCZ which is beneficial in multiuser environment to resist inter-cell interference caused by users from different cells in CDMA systems.*

## APPENDIX A

### PROOF OF *Theorem 1*

We first state and prove a lemma which will later be used to prove the *Theorem 1*.

*Lemma 3:* For two non-negative integers  $i$  and  $j$ , let  $(i_1, i_2, \dots, i_m)$  and  $(j_1, j_2, \dots, j_m)$  be  $p$ -ary representation of  $i$  and  $j$  respectively. Let  $f : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_\lambda$  be a function as defined in (15).

Now, we can write  $a_{\mathbf{u}_k}^{\mathbf{v}_k}$  by using (16) and (17) as

$$a_{\mathbf{u}_k}^{\mathbf{v}_k} = f + \frac{\lambda}{p} \sum_{\beta=1}^k x_{\pi_\beta(1)} u_\beta + \frac{\lambda}{p} \sum_{\beta=1}^k x_{\pi_\beta(n_\beta)} v_\beta. \quad (31)$$

Further, suppose we have  $i_{\pi_\beta(1)} = j_{\pi_\beta(1)} \forall \beta = 1, 2, \dots, k$ . For a certain  $\beta' \leq k$ , let us assume  $t$  be the smallest integer such that  $i_{\pi_{\beta'}(t)} \neq j_{\pi_{\beta'}(t)}$ . Let us define  $i^\eta$  to be an integer whose vector representation with base  $p$  is

$$(i_1, i_2, \dots, i_{\pi_{\beta'}(t-1)} - \eta, \dots, i_m), \quad (32)$$

which differs from that of  $i$  only at the position  $\pi_{\beta'}(t-1)$  and  $\eta = 1, 2, \dots, (p-1)$ . Similarly, we define  $j^\eta$  such that its vector representation with base  $p$  is

$$(j_1, j_2, \dots, j_{\pi_{\beta'}(t-1)} - \eta, \dots, j_m). \quad (33)$$

Then we have

$$\sum_{\eta=1}^{p-1} \omega_\lambda^{(a_{\mathbf{u}_k}^{\mathbf{v}_k})_{j^\eta} - (a_{\mathbf{u}_k}^{\mathbf{v}_k})_{i^\eta}} + \omega_\lambda^{(a_{\mathbf{u}_k}^{\mathbf{v}_k})_{j^\eta} - (a_{\mathbf{u}_k}^{\mathbf{v}_k})_{i^\eta}} = 0. \quad (34)$$

*Proof:* For notational convenience, we write  $a_{\mathbf{u}_k}^{\mathbf{v}_k} = \mathbf{c}$ . Now using (15) and (31), we can write

$$\begin{aligned} \mathbf{c}_{i^\eta} - \mathbf{c}_i &= f_{i^\eta} - f_i \\ &= \frac{\lambda}{p} [i_{\pi_{\beta'}(t-2)} i_{\pi_{\beta'}(t-1)}^\eta + i_{\pi_{\beta'}(t-1)}^\eta i_{\pi_{\beta'}(t)} - i_{\pi_{\beta'}(t-2)} i_{\pi_{\beta'}(t-1)}^\eta - i_{\pi_{\beta'}(t-1)} i_{\pi_{\beta'}(t)}] \\ &\quad + g_{\pi_{\beta'}(t-1)} [i_{\pi_{\beta'}(t-1)}^\eta - i_{\pi_{\beta'}(t-1)}] \\ &= [-\eta \frac{\lambda}{p} i_{\pi_{\beta'}(t)} - \eta \frac{\lambda}{p} i_{\pi_{\beta'}(t-2)} - \eta g_{\pi_{\beta'}(t-1)}] \\ &= -\eta [\frac{\lambda}{p} i_{\pi_{\beta'}(t)} + \frac{\lambda}{p} i_{\pi_{\beta'}(t-2)} + g_{\pi_{\beta'}(t-1)}]. \end{aligned} \quad (35)$$

Similarly,

$$\mathbf{c}_{j^\eta} - \mathbf{c}_j = f_{j^\eta} - f_j = -\eta [\frac{\lambda}{p} j_{\pi_{\beta'}(t)} + \frac{\lambda}{p} j_{\pi_{\beta'}(t-2)} + g_{\pi_{\beta'}(t-1)}]. \quad (36)$$

From (35) and (36), we have

$$(\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta}) - (\mathbf{c}_i - \mathbf{c}_j) = -\eta \frac{\lambda}{p} (i_{\pi_{\beta'}(t)} - j_{\pi_{\beta'}(t)}). \quad (37)$$

Now, taking sum of  $\omega_\lambda^{(\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta}) - (\mathbf{c}_i - \mathbf{c}_j)}$  over  $\eta$ , we have

$$\sum_{\eta=1}^{p-1} \omega_\lambda^{\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta} - (\mathbf{c}_i - \mathbf{c}_j)} = \sum_{\eta=1}^{p-1} \omega_\lambda^{\eta \frac{\lambda}{p} (j_{\pi_{\beta'}(t)} - i_{\pi_{\beta'}(t)})} = \sum_{\eta=1}^{p-1} \omega_p^{\eta(j_{\pi_{\beta'}(t)} - i_{\pi_{\beta'}(t)})}. \quad (38)$$

It is given that  $i_{\pi_{\beta'}(t)} \neq j_{\pi_{\beta'}(t)}$ , implies that  $i_{\pi_{\beta'}(t)} - j_{\pi_{\beta'}(t)} \neq 0$  and hence RHS of (38) is the sum of roots of polynomial  $z^p - 1 = 0$  except the root  $z = 1$ . Hence

$$\sum_{\eta=1}^{p-1} \omega_p^{\eta(j_{\pi_{\beta'}(t)} - i_{\pi_{\beta'}(t)})} = -1. \quad (39)$$

Therefore, from (38) and (39), we have

$$\sum_{\eta=1}^{p-1} \omega_\lambda^{\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta} - (\mathbf{c}_i - \mathbf{c}_j)} = -1, \quad (40)$$

which further implies that

$$\sum_{\eta=1}^{p-1} \omega_\lambda^{\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta}} + \omega_\lambda^{(\mathbf{c}_i - \mathbf{c}_j)} = 0. \quad (41)$$

■

*Proof of Theorem 1:* We need to show that for a fixed  $\mathbf{u}_k$ ,  $\mathbf{C}_{\mathbf{u}_k}$  is a  $(p^k, (p-1)p^{\pi_1(2)-1}, p^m)$ -ZCZ. Except the ZCZ width all the parameters are directly inherited from *Lemma 2*. So, we only need to show that the ZCZ width is  $(p-1)p^{\pi_1(2)-1}$ . Let  $\mathbf{c} \in \mathbf{C}_{\mathbf{u}_k}$ , by (18),  $\mathbf{c} = \psi(a_{\mathbf{u}_k}^{\mathbf{v}_{k_1}})$  for some  $0 \leq \mathbf{v}_{k_1} \leq p^k - 1$ . First, we find the PACF of  $\mathbf{c}$  and show that for  $0 < \tau \leq (p-1)p^{\pi_1(2)-1}$ ,

$$\mathcal{P}(\mathbf{c})(\tau) = \sum_{i=0}^{L-1} \omega_\lambda^{\mathbf{c}_{(i+\tau) \bmod L} - \mathbf{c}_i} = 0, \quad (42)$$

where  $L$  is the length of the sequence, i.e.,  $L = p^m$ . For any integer  $i$ , let us denote another integer  $j = (i + \tau) \bmod L$ . Then we consider two cases and demonstrate that for each pair  $(i, j)$  there exist other  $(p-1)$  pairs  $(i^\eta, j^\eta)$ ,  $\eta = 1, 2, \dots, p-1$  such that

$$\sum_{\eta=1}^{p-1} \omega_\lambda^{\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta}} + \omega_\lambda^{(\mathbf{c}_i - \mathbf{c}_j)} = 0, \quad (43)$$

in each case.

*Case 1* ( $i_{\pi_1(2)} = j_{\pi_1(2)}$ ): In this case, we have  $i_{\pi_\beta(1)} = j_{\pi_\beta(1)}$ ,  $\forall \beta = 1, 2, \dots, k$ . For the contrary, suppose this is not true. Then, assume that  $\bar{\beta}$  is the largest integer such that  $i_{\pi_{\bar{\beta}}(1)} \neq j_{\pi_{\bar{\beta}}(1)}$ . For ease of presentation, let  $d = \pi_{\bar{\beta}}(1)$ , now if  $j_d > i_d$ , we have

$$\begin{aligned}
\tau = j - i &= \sum_{s=1}^d (j_s - i_s)p^{s-1} \\
&= (j_d - i_d)p^{d-1} + \sum_{s=1, s \neq \pi_1(2)}^{d-1} (j_s - i_s)p^{s-1} \\
&\geq (j_d - i_d)p^{d-1} - (p-1) \sum_{s=1}^{d-1} p^{s-1} + (p-1)p^{\pi_1(2)-1} \\
&= (j_d - i_d)p^{d-1} - (p-1) \left[ \frac{p^{d-1} - 1}{p-1} \right] + (p-1)p^{\pi_1(2)-1} \\
&= (j_d - i_d - 1)p^{d-1} + 1 + (p-1)p^{\pi_1(2)-1} > (p-1)p^{\pi_1(2)-1}. \tag{44}
\end{aligned}$$

Hence (44) implies that  $\tau > (p-1)p^{\pi_1(2)-1}$  which is a contradiction. Similarly, if  $j_d < i_d$ , then

$$\begin{aligned}
\tau = j - i + p^m &= \sum_{s=1}^d (j_s - i_s)p^{s-1} + p^m \\
&= (j_d - i_d)p^{m-\bar{\beta}} + p^m + \sum_{s=1, s \neq \pi_1(2)}^{d-1} (j_s - i_s)p^{s-1} \\
&= (j_d - i_d + p^{\bar{\beta}})p^{m-\bar{\beta}} + \sum_{s=1, s \neq \pi_1(2)}^{d-1} (j_s - i_s)p^{s-1} \\
&\geq (j_d - i_d + p^{\bar{\beta}})p^{m-\bar{\beta}} - (p-1) \sum_{s=1}^{d-1} p^{s-1} + (p-1)p^{\pi_1(2)-1} \\
&= (j_d - i_d + p^{\bar{\beta}} - 1)p^{m-\bar{\beta}} + 1 + (p-1)p^{\pi_1(2)-1} > (p-1)p^{\pi_1(2)-1}. \tag{45}
\end{aligned}$$

Again we got a contradiction. Hence  $i_{\pi_\beta(1)} = j_{\pi_\beta(1)} \forall \beta = 1, 2, \dots, k$ . Now without loss of generality, we assume that there exist a positive integer  $\beta' \leq k$  such that  $i_{\pi_{\beta'}(r)} = j_{\pi_{\beta'}(r)}$ ,  $\forall \beta = 1, 2, \dots, \beta' - 1$  and  $r = 1, 2, \dots, n_{\beta'}$ . Assume  $t$  be the smallest integer with  $i_{\pi_{\beta'}(t)} \neq j_{\pi_{\beta'}(t)}$ . Now,

let us define  $i^\eta$  and  $j^\eta$  same as in (32) and (33) respectively. Then it can easily be obtained that  $j^\eta = (i^\eta + \tau) \bmod L$  and hence using *Lemma 3*, we get (43).

*Case 2* ( $i_{\pi_1(2)} \neq j_{\pi_1(2)}$ ): In this case, let  $i^\eta$  and  $j^\eta$  are modified from  $i$  and  $j$  by changing only last bit of  $i$  and  $j$  as  $i_m^\eta = i_m - \eta$  and  $j_m^\eta = j_m - \eta$ . Then

$$\begin{aligned} \mathbf{c}_{i^\eta} - \mathbf{c}_i &= f_{i^\eta} - f_j + \frac{\lambda}{p}(i_m - \eta - i_m)u_1 \\ &= \frac{\lambda}{p} [i_m^\eta i_{\pi_1(2)} - i_m i_{\pi_1(2)}] + g_m(i_m - \eta - i_m) + \frac{\lambda}{p}(i_m - \eta - i_m)u_1 \\ &= -\eta \left[ \frac{\lambda}{p} i_{\pi_1(2)} + g_m + \frac{\lambda}{p} u_1 \right]. \end{aligned} \quad (46)$$

Similarly,

$$\mathbf{c}_{j^\eta} - \mathbf{c}_j = -\eta \left[ \frac{\lambda}{p} j_{\pi_1(2)} + g_m + \frac{\lambda}{p} u_1 \right]. \quad (47)$$

By subtracting (47) from (46), we get

$$(\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta}) - (\mathbf{c}_i - \mathbf{c}_j) = -\eta \frac{\lambda}{p} (i_{\pi_1(2)} - j_{\pi_1(2)}). \quad (48)$$

Now following the same steps as in (37), (38), (39), and (40), we get

$$\sum_{\eta=1}^{p-1} \omega_\lambda^{\mathbf{c}_{i^\eta} - \mathbf{c}_{j^\eta}} + \omega_\lambda^{\mathbf{c}_i - \mathbf{c}_j} = 0. \quad (49)$$

Till now we have proved that for  $0 < \tau \leq (p-1)p^{\pi_1(2)-1}$ , the value of  $\mathcal{P}(\mathbf{c})(\tau) = 0$ . Now in the rest of the proof, we will prove that for any  $0 \leq \tau \leq (p-1)p^{\pi_1(2)-1}$ , the PCCF of any two different sequences in  $\mathbf{C}_{\mathbf{u}_k}$  is zero. For that let  $0 \leq \gamma_k, \delta_k \leq p^k - 1$  such that  $\psi(a_{\mathbf{u}_k}^{\gamma_k}), \psi(a_{\mathbf{u}_k}^{\delta_k}) \in \mathbf{C}_{\mathbf{u}_k}$ . Again for notational convenience, we denote  $\psi(a_{\mathbf{u}_k}^{\gamma_k})$  and  $\psi(a_{\mathbf{u}_k}^{\delta_k})$  by  $\mathbf{b}$  and  $\mathbf{c}$  respectively. Then, we need to prove that for  $0 \leq \tau \leq (p-1)p^{\pi_1(2)-1}$ ,

$$\mathcal{P}(\mathbf{c}, \mathbf{b})(\tau) = \sum_{i=0}^{L-1} \omega_\lambda^{\mathbf{c}_{(i+\tau) \bmod L} - \mathbf{b}_i} = 0. \quad (50)$$

Let  $j = (i + \tau) \bmod L$ . Following similar arguments as in *Case 1* and *Case 2*, for any pair  $(i, j)$ , we can find other pairs  $(i^\eta, j^\eta)$ ,  $\eta = 1, 2, \dots, k-1$  such that

$$\sum_{\eta=1}^{p-1} \omega_\lambda^{\mathbf{c}_{i^\eta} - \mathbf{b}_{j^\eta}} + \omega_\lambda^{\mathbf{c}_i - \mathbf{b}_j} = 0, \quad (51)$$

for  $\tau \neq 0$ , where  $j^\eta = (i^\eta + \tau) \bmod L$ . Therefore, we can obtain that (50) holds for  $\tau \neq 0$ . Now, it remains to prove that,

$$\mathcal{P}(\mathbf{c}, \mathbf{b})(0) = \sum_{i=0}^{L-1} \omega_\lambda^{c_i - \mathbf{b}_i} = 0. \quad (52)$$

Taking (31) into consideration, let  $\mathbf{c} - \mathbf{b} = \frac{\lambda}{p} \cdot \mathbf{d}$ . Then  $\mathbf{d}$  is a non-zero codeword in  $GRM_p(1, m)$ . Now let  $\mathbf{d} = (d_1, d_2, \dots, d_{p^m})$  and hence  $\mathbf{d}$  can be written as linear combination of  $\theta(x_1), \theta(x_2), \dots, \theta(x_m)$  as  $\mathbf{d} = c_1 \cdot \theta(x_1) + c_2 \cdot \theta(x_2) + \dots + c_m \cdot \theta(x_m)$ , where  $c_i \in \mathbb{Z}_p$ ,  $1 \leq i \leq m$ . For each  $i$ ,  $\theta(x_i)$  contains each element of the set  $\{0, 1, \dots, p-1\}$ ,  $p^{m-1}$  times. Hence  $\mathbf{d}$  will also contains each element of the set  $\{0, 1, \dots, p-1\}$ ,  $p^{m-1}$  times. Now (52) can be written as

$$\mathcal{P}(\mathbf{c}, \mathbf{b})(0) = \sum_{i=0}^{L-1} \omega_\lambda^{\frac{\lambda}{p} \mathbf{d}_i} = \sum_{i=0}^{L-1} \omega_\lambda^{\frac{\lambda}{p} \mathbf{d}_i} = \sum_{i=0}^{L-1} \omega_p^{\mathbf{d}_i} = 0. \quad (53)$$

Hence the *Theorem 1* is proved. ■

## REFERENCES

- [1] M. Golay, "Complementary series," *IRE Trans. on Inf. Theory*, vol. 7, no. 2, pp. 82–87, 1961.
- [2] C.-C. Tseng and C. Liu, "Complementary sets of sequences," *IEEE Trans. on Inf. Theory*, vol. 18, no. 5, pp. 644–652, 1972.
- [3] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. on inf. theory*, vol. 45, no. 7, pp. 2397–2417, 1999.
- [4] K. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. on Inf. Theory*, vol. 46, no. 1, pp. 104–120, 2000.
- [5] C. Han, N. Suehiro, and T. Hashimoto, "N-shift cross-orthogonal sequences and complete complementary codes," in *2007 IEEE Int. Symp. on Inf. Theory*, 2007, pp. 2611–2615.
- [6] S.-M. Tseng and M. Bell, "Asynchronous multicarrier DS-CDMA using mutually orthogonal complementary sets of sequences," *IEEE Trans. on Commun.*, vol. 48, no. 1, pp. 53–59, 2000.
- [7] H.-H. Chen, J.-F. Yeh, and N. Suehiro, "A multicarrier CDMA architecture based on orthogonal complementary codes for new generations of wideband wireless communications," *IEEE Commun. Mag.*, vol. 39, no. 10, pp. 126–135, 2001.
- [8] 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, 2007.

- [9] S. Li, J. Chen, and L. Zhang, "Optimisation of complete complementary codes in MIMO radar system," *Electron. Lett.*, vol. 46, pp. 1157–1159, 2010.
- [10] J. Tang, N. Zhang, Z. Ma, and B. Tang, "Construction of doppler resilient complete complementary code in MIMO radar," *IEEE Trans. Signal Process.*, vol. 62, no. 18, pp. 4704–4712, 2014.
- [11] 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," in *IEEE Int. Conf. Commun.*, 2008, pp. 4840–4844.
- [12] T. Kojima, T. Tachikawa, A. Oizumi, Y. Yamaguchi, and U. Parampalli, "A disaster prevention broadcasting based on data hiding scheme using complete complementary codes," in *Int. Symp. Inf. Theory Appl. (ISITA)*, 2014, pp. 45–49.
- [13] A. Rathinakumar and A. Chaturvedi, "Complete mutually orthogonal Golay complementary sets from Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 54, pp. 1339 – 1346, 2008.
- [14] P. Sarkar, Z. Liu, and S. Majhi, "A direct construction of complete complementary codes with arbitrary lengths," *CoRR*, vol. abs/2102.10517, 2021.
- [15] Z. Wang, G. Wu, and D. Ma, "A new method to construct Golay complementary set by paraunitary matrices and Hadamard matrices," *arXiv preprint arXiv:1910.10302*, 2019.
- [16] Z. Wang, E. Xue, and J. Chai, "A method to construct complementary sets of non-power-of-two length by concatenation," in *2017 Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA)*, 2017, pp. 24–28.
- [17] Z. Wang, D. Ma, G. Gong, and E. Xue, "New construction of complementary sequence (or array) sets and complete complementary codes," *IEEE Trans. on Inf. Theory*, vol. 67, no. 7, pp. 4902–4928, 2021.
- [18] C.-Y. Chen, C.-H. Wang, and C.-C. Chao, "Complete complementary codes and generalized Reed-Muller codes," *IEEE Commun. Lett.*, vol. 12, no. 11, pp. 849–851, 2008.
- [19] P. Kumar, S. Majhi, and S. Paul, "A direct construction of GCP and binary CCC of length non power of two," *arXiv preprint arXiv:2109.08567*, 2021.
- [20] P. Spasojevic and C. Georghiades, "Complementary sequences for ISI channel estimation," *IEEE Trans. on Inf. Theory*, vol. 47, no. 3, pp. 1145–1152, 2001.
- [21] J. Groenewald and B. Maharaj, "MIMO channel synchronization using Golay complementary pairs," in *AFRICON 2007*. IEEE, 2007, pp. 1–5.
- [22] Y. Wang, T. Hu, Y. Yang, and Z. Zhou, "Large zero correlation zones of Golay complementary sets," in *2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA)*, 2019, pp. 1–5.
- [23] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. on Veh. Technol.*, vol. 47, no. 4, pp. 1268–1275, 1998.
- [24] H. Haderer, R. Feger, C. Pfeffer, and A. Stelzer, "Millimeter-wave phase-coded CW MIMO radar using zero- and low-correlation-zone sequence sets," *IEEE Trans. Microw. Theory and Techn.*, vol. 64, no. 12, pp. 4312–4323, 2016.

- [25] S. Hu, Z. Liu, Y. L. Guan, C. Jin, Y. Huang, and J.-M. Wu, "Training sequence design for efficient channel estimation in MIMO-FBMC systems," *IEEE Access*, vol. 5, pp. 4747–4758, 2017.
- [26] S.-A. Yang and J. Wu, "Optimal binary training sequence design for multiple-antenna systems over dispersive fading channels," *IEEE Trans. Veh. Technol.*, vol. 51, no. 5, pp. 1271–1276, 2002.
- [27] W. Yuan, P. Wang, and P. Fan, "Performance of multi-path MIMO channel estimation based on ZCZ training sequences," in *IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications*, vol. 2, 2005, pp. 1542–1545 Vol. 2.
- [28] R. Zhang, X. Cheng, M. Ma, and B. Jiao, "Interference-avoidance pilot design using ZCZ sequences for multi-cell MIMO-OFDM systems," in *IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 5056–5061.
- [29] W. Zhang, F. Zeng, X. Long, and M. Xie, "Improved mutually orthogonal ZCZ polyphase sequence sets and their applications in OFDM frequency synchronization," in *6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, 2010, pp. 1–5.
- [30] J.-D. Yang, X. Jin, K.-Y. Song, J.-S. No, and D.-J. Shin, "Multicode MIMO systems with quaternary LCZ and ZCZ sequences," *IEEE Trans. on vehicular technology*, vol. 57, no. 4, pp. 2334–2341, 2008.
- [31] S. He, Y. Huang, S. Jin, and L. Yang, "Coordinated beamforming for energy efficient transmission in multicell multiuser systems," *IEEE Trans. on Commun.*, vol. 61, no. 12, pp. 4961–4971, 2013.
- [32] C. Fragouli, N. Al-Dhahir, and W. Turin, "Training-based channel estimation for multiple-antenna broadband transmissions," *IEEE Trans. on Wireless Commun.*, vol. 2, no. 2, pp. 384–391, 2003.
- [33] X. Deng and P. Fan, "Spreading sequence sets with zero correlation zone," *Electronics Letters*, vol. 36, pp. 993 – 994, 2000.
- [34] R. Appuswamy and A. Chaturvedi, "A new framework for constructing mutually orthogonal complementary sets and zero correlation zone sequences," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3817 – 3826, 2006.
- [35] X. Tang, P. Fan, and J. Lindner, "Multiple binary zero correlation zone sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Trans. Inf. Theory*, vol. 56, pp. 4038 – 4045, 2010.
- [36] Y.-C. Liu, C.-W. Chen, and Y. T. Su, "New constructions of zero-correlation zone sequences," *IEEE Trans. on Inf. Theory*, vol. 59, no. 8, pp. 4994–5007, 2013.
- [37] Z. Zhou, X. Tang, and G. Gong, "A new class of sequences with zero or low correlation zone based on interleaving technique," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4267 – 4273, 2008.
- [38] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Trans. Inf. Theory*, vol. 50, pp. 559 – 565, 2004.
- [39] Y. S. Tang, C. Y. Chen, and C. C. Chao, "A novel construction of zero correlation zone sequences based on Boolean functions," in *IEEE 11th International Symposium on Spread Spectrum Techniques and Applications*, 2010, pp. 198–203.
- [40] Z. Liu, Y. Guan, and U. Paramalli, "A new construction of zero correlation zone sequences from generalized Reed-Muller codes," in *IEEE Inf. Theory Workshop (ITW)*, 2014.

- [41] N. Kumar, S. Majhi, P. Sarkar, and A. K. Upadhyay, “A direct construction of prime-power-length zero-correlation zone sequences for QS-CDMA system,” 2021. [Online]. Available: <https://arxiv.org/abs/2111.06675>
- [42] G. Gong, F. Huo, and Y. Yang, “Large zero autocorrelation zones of Golay sequences and their applications,” *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3967–3979, 2013.
- [43] —, “Large zero correlation zone of Golay pairs and QAM Golay pairs,” in *2013 IEEE Int. Symp. on Inf. Theory*, 2013, pp. 3135–3139.
- [44] C.-Y. Chen and S.-W. Wu, “Golay complementary sequence sets with large zero correlation zones,” *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5197–5204, 2018.
- [45] Z. Gu, Z. Zhou, A. R. Adhikary, Y. Feng, and P. Fan, “Asymptotically optimal Golay-ZCZ sequence sets with flexible length,” 2021. [Online]. Available: <https://arxiv.org/abs/2112.08678>
- [46] —, “Construction of Golay-ZCZ sequences with new lengths,” in *IEEE Int. Symp. on Inf. Theory (ISIT)*, 2021, pp. 1802–1805.
- [47] —, “New constructions of Golay complementary pair/array with large zero correlation zone,” 2021. [Online]. Available: <https://arxiv.org/abs/2108.05657>
- [48] A. R. Adhikary, Z. Liu, Y. L. Guan, S. Majhi, and S. Z. Budishin, “Optimal binary periodic almost-complementary pairs,” *IEEE Signal Processing Letters*, vol. 23, no. 12, pp. 1816–1820, 2016.
- [49] P. Sarkar, S. Majhi, and Z. Liu, “A direct and generalized construction of polyphase complementary sets with low PMEPR and high code-rate for OFDM system,” *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6245–6262, 2020.
- [50] X. Tang, P. Fan, and S. Matsufuji, “Lower bounds on correlation of spreading sequence set with low or zero correlation zone,” *Electronics Letters*, vol. 36, pp. 551 – 552, 2000.
- [51] S. Matsufuji, “Spreading sequence set for approximately synchronized CDMA system with no co-channel interference and high data capacity,” *WPMC’*, pp. 333–339, 1999.
- [52] T. Kasami, S. Lin, and W. Peterson, “New generalizations of the Reed-Muller codes-I: Primitive codes,” *IEEE Trans. on Inf. Theory*, vol. 14, no. 2, pp. 189–199, 1968.
- [53] D. Zhang, M. Parker, and T. Hellesteth, “Polyphase zero correlation zone sequences from generalised Bent functions,” *Cryptography and Commun.*, vol. 12, pp. 1–11, 2020.
- [54] Z. Zhou, D. Zhang, T. Hellesteth, and J. Wen, “A construction of multiple optimal zero correlation zone sequence sets with good cross-correlation,” *IEEE Trans. Inf. Theory*, vol. PP, pp. 1–1, 2018.
- [55] T. Hayashi, “A class of zero-correlation zone sequence set using a perfect sequence,” *IEEE Signal Process. Lett.*, vol. 16, pp. 331 – 334, 2009.
- [56] Z. Liu, Y. L. Guan, and U. Paramalli, “New complete complementary codes for peak-to-mean power control in multi-carrier CDMA,” *IEEE Trans. on Commun.*, vol. 62, no. 3, pp. 1105–1113, 2014.
- [57] S.-W. Wu and C.-Y. Chen, “Optimal Z-complementary sequence sets with good peak-to-average power-ratio property,” *IEEE Signal Process. Lett.*, vol. 25, no. 10, pp. 1500–1504, 2018.