A Direct Construction of GCP and Binary CCC of Length Non-Power of Two
Praveen Kumar, Sudhan Majhi, Subhabrata Paul

Abstract—Golay complementary pairs (GCPs) and complete complementary codes (CCCs) have found a wide range of practical applications in coding, signal processing and wireless communication due to their ideal correlation properties. In fact, binary CCCs have special advantages in spread spectrum communication due to their simple modulo-2 arithmetic operation, modulation and correlation simplicity, but they are limited in length. In this paper, we present a direct construction of GCPs, mutually orthogonal complementary sets (MOCSs) and binary CCCs of non-power of two lengths to widen their application in the recent field. First, a generalised Boolean function (GBF) based truncation technique has been used to construct GCPs of non-power of two lengths. Then Complementary sets (CSs) and MOCSs of lengths of the form $2^{m-1} + 2^{m-3}$ ($m \geq 5$) and $2^{m-1} + 2^{m-2} + 2^{m-3}$ ($m \geq 6$) are generated by GBFs. Finally, binary CCCs with desired lengths are constructed using the union of MOCSs. The row and column sequence peak to mean envelope power ratio (PMEPR) has been investigated and compared with existing work. The column sequence PMEPR of resultant CCCs can be effectively upper bounded by 2.

Index Terms—Complementary set (CS), complete complementary set (CCC), generalised Boolean function (GBF), Golay complementary pair (GCP), mutually orthogonal complementary set (MOCS)

I. INTRODUCTION

THE Golay complementary pairs (GCPs) were first introduced by Golay [1]. The aperiodic auto-correlation sum (AACS) of a GCP diminishes to zero for all time shifts except at zero. The sequences in a GCP are known as Golay sequences. The idea of GCP is further extended to the complementary set (CS) by Tseng and Liu [2]. A CS is a set of $M(\geq 2)$ sequences of length $N$ with the property that their AACS sum is zero for all non-zero time shifts. Tseng and Liu also proposed the concept of $(K, M, N)$-mutually orthogonal complementary set (MOCS), which is a collection of $K$ CSs each of having $M$ sequences of length $N$, such that any two distinct CSs are orthogonal to each other, and follows the property $K \leq M$ [3]. For a special case, when the set size of MOCS achieves its upper bound, i.e., $K = M$, it is known as a set of complete complementary code (CCC) and is denoted by $(K, K, N)$-CCC [4]. Due to the ideal correlation properties and optimal set size, CCCs have found their application in next-generation multi-carrier code division multiple access (MC-CDMA) [5]–[9]. Apart from this, CCCs are utilized in optimal channel estimation in multiple-input and multiple-output (MIMO) frequency-selective fading channels [10], MIMO radar [11], [12], cell search in orthogonal frequency division multiplexing (OFDM) systems [13], and data hiding [14]. In spread spectrum communication, the binary CCC is preferred compared to non-binary CCC due to its simple modulo-2 arithmetic operation, modulation and correlation simplicity.

Due to modulo-2 arithmetic operation, binary sequences are easy to implement electronically. The modulo-2 arithmetic is isomorphic with the use of $\{\pm 1\}$ which simplifies both the modulation and correlation processes. However, it is difficult in many cases to get flexible lengths for binary sequences. It has been proved in [15] that binary GCPs exist for only even length. Binary Z-complementary pairs (ZCPs) were introduced by Fan et al. in [16] and they also proved that ZCPs exists for all possible lengths. Several constructions of binary ZCPs of different lengths are proposed in [17], [18]. Construction of binary CSs of non-power of two lengths can be found in [19].

In the year 1999, Davis and Jedwab have proposed a direct construction of $2^h$-ary ($h \in \mathbb{N}$) GCPs of length $2^m$ ($m \in \mathbb{N}$) using generalised Boolean functions (GBFs) [20]. Paterson extended the idea of $2^h$-ary GCPs to $q$-ary (for even $q$) GCPs [21]. The construction of GCPs of length $2^n103267$ ($\alpha, \beta, \gamma \in \mathbb{N}$) is provided by using repeated application of Turyn’s construction [22]. In [21], Paterson has also proposed a GBFs based construction of CSs of length $2^m$. In the recent development GBFs based construction of CSs with more flexible lengths have been proposed in [23]–[27]. CSs with flexible lengths are of interest to OFDM systems where numbers of subcarriers are varied, i.e., non-power of two adopted by the LTE system. A direct and generalised construction of polyphase CSs is proposed in [28] and it has low peak to mean envelope power ratio (PMEPR).

In [29], Rathinakumar and Chaturvedi proposed a direct construction of CCCs of length $2^m$ by extending the Paterson’s idea of CSs generation. A number of direct constructions of CCCs with lengths $2^m$ are presented in [8], [30]–[32]. Several GBFs based constructions of Z-complementary code sets (ZCCSs) of non-power of two lengths are proposed in the literature [33]–[38], to extend the number of users in ZCCS based MC-CDMA system compared to that of CCC based MC-CDMA system. Apart from the GBFs based construction, MOCSs with non-power of two lengths can be constructed by using different systematic methods, which include reversals, negations, interleaving, concatenations etc. [2], [39]. In the same way, Das et al. presented the construction of MOCSs and binary CCCs of different lengths by using paraunitary (PU)
We can also define the ACCF and AACF of $\mathbb{Z}_q$ valued sequences by defining a one-one correspondence between $\mathbb{Z}_q$ valued sequence $\mathbf{e} = (e_0, e_1, \ldots, e_{N-1})$ and the complex-valued sequence $\mathbf{e}' = (e_0', e_1', \ldots, e_{N-1}')$, where $e_i' = \omega^{e_i}$, and $\omega = \exp (2\pi \sqrt{-1}/q)$ is $q$th root of unity. So if $\mathbf{d}$ and $\mathbf{e}$ are $\mathbb{Z}_q$ valued sequences then we define their ACCF $\mathcal{C}(\mathbf{d}, \mathbf{e})(s)$ and AACF $\mathcal{A}(\mathbf{e})(s)$ respectively as ACCF and AACF of the corresponding complex-value sequence $\mathbf{d}' = \mathbf{e}'$.

**Definition 2:** A set of $M$ sequences $e_0, e_1, \ldots, e_{M-1}$, each of length $N$, is said to be a CS if

$$\mathcal{A}(e_0)(s) + \mathcal{A}(e_1)(s) + \cdots + \mathcal{A}(e_{M-1})(s) = \begin{cases} MN, & s = 0, \\ 0, & \text{otherwise.} \end{cases}$$

For $M = 2$, it is known as a GCP.

**Definition 3:** Consider a set $E = \{E^0, E^1, \ldots, E^{K-1}\}$, where each set $E^p$ consists of $M$ sequences, i.e., $E^p = \{e_{0}^{p0}, e_{1}^{p0}, \ldots, e_{M-1}^{p0}\}$, and length of each sequence $e_{0}^{p0}$ is $N$, where $0 \leq p \leq K - 1$ and $0 \leq l \leq M - 1$. The set $E$ is called an MOCS, denoted by $(K, M, N)$-MOCS, if the ACCF of $E^p$ and $E^{p'}$ satisfies

$$\mathcal{C}(E^p, E^{p'})(s) = \sum_{n=0}^{M-1} \mathcal{C}(e_{n}^{p0}, e_{n}^{p'0})(s) = \begin{cases} MN, & s = 0, p = p', \\ 0, & \text{otherwise.} \end{cases}$$

where $0 \leq p, p' \leq K - 1; K, M$ and $N$ are known as the set size, flock size and sequence length respectively. For a $(K, M, N)$-MOCS, the set size is always smaller than the flock size, i.e., $K \leq M$. For the special case when $K = M$, the MOCS is called a CCC of order $K$ and length $N$, and is denoted by $(K, K, N)$-CCC.

**A. Generalised Boolean function**

A GBF $f$ in $m$ binary variables $y_0, y_1, \ldots, y_{m-1}$ is a function from $\{0, 1\}^m$ to $\mathbb{Z}_q$, where $q \geq 2$ is an even integer. A monomial of degree $r$ is defined as the product of any $r$ variables among $y_0, y_1, \ldots, y_{m-1}$. So there are $\sum_{r=0}^{m} \binom{m}{r} = 2^m$ monomials, namely $1, y_0, y_1, \ldots, y_{m-1}, y_0y_1, y_0y_2, \ldots, y_{m-2}y_{m-1}, \ldots, y_0y_1 \cdots y_{m-1}$.

With the linear combination of these $2^m$ monomials and by taking coefficient from $\mathbb{Z}_q$, a GBF can be expressed uniquely. In the expression of a GBF of order $r$, there exist at least one highest-degree monomial of order $r$ with non-zero coefficient. Corresponding to a GBF $f$ of $m$ variables $y_0, y_1, \ldots, y_{m-1}$, length $2^m \mathbb{Z}_q$-valued vector is expressed as

$$f = (f_0, f_1, \ldots, f_{2^m-1}),$$

where $f_i = f(i_0, i_1, \ldots, i_{m-1})$ and $(i_0, i_1, \ldots, i_{m-1})$ is the binary vector representation of $i$. A complex-valued vector $f'$ is associated with every $f$ by $f'_i = \omega^{f_i}$. When it is clear from the context, only $f$ is used to refer to both. Corresponding to a GBF $f$ with $m$ variables the sequence $f$ is of length $2^m$.

We can restrict the domain of GBF to get sequences of length non-power of two. Let us define a set $A$ which is a
subset of \( \{0,1\}^m \). So, depending upon the domain \( A \) we can get different length sequences corresponding to GBF \( f \). By \( a_m \) we mean the binary vector representation of positive integer \( m \) in \( m \) components.

**Example 1:** Let \( f : A \to \mathbb{Z}_q \) be defined as \( f(y_0, y_1, y_2) = y_0y_1 + y_2 \), where \( A = \{0_1, 13, \ldots, 5_3\} \), then the sequence corresponding to \( f \) is \((1,1,1,-1,-1,-1)\), which is of length 6. Similarly, if we define \( A = \{3_3, 4_3, \ldots, 7_3\} \), then we get the sequence \((-1, -1, -1, -1, -1, -1)\), which is of length 5.

**B. Graph of Quadratic form of GBF**

Let \( Q : \{0,1\}^m \to \mathbb{Z}_q \) be a GBF of order 2 defined by

\[
Q(y_0, y_1, \ldots, y_{m-1}) = \sum_{0 \leq i < j < k} q_{ij} y_i y_j,
\]

where \( k \leq m \) and \( q_{ij} \in \mathbb{Z}_q \). We associate a labeled graph \( G(Q) \) corresponding to the GBF \( Q \), on \( k \) vertices by representing the vertices of \( G(Q) \) by \( 0, 1, \ldots, m-1 \) and joining two vertices \( i \) and \( j \) by an edge labeled \( q_{ij} \) if and only if \( q_{ij} \neq 0 \). In the case, \( q = 2 \), \( g_{ij} \) can only take values either 0 or 1, so every edge is labelled 1 and by convention, edge labels are omitted in this case. From any given graph \( G(Q) \) of this type, the quadratic form \( Q \) can be easily and uniquely recovered. A graph \( G(Q) \) is called a path on \( k \) vertices if the number of edges is exactly less than the number of vertices, and each edge is labelled \( q/2 \). For \( k = 1 \), this is a trivial path and for \( k \geq 2 \), this type of path is known as the Hamiltonian path. For \( 2 \leq k < m \), a path on \( k \) vertices corresponds to a quadratic form of the type

\[
Q = \sum_{0 \leq i < j < k} q_{ij} y_i y_j,
\]

where \( q \) is a permutation of the set \( \{0,1,\ldots,k-1\} \).

**C. Restricted Boolean function**

Let \( f : A \subseteq \{0,1\}^m \to \mathbb{Z}_q \) be a GBF in variables \( y_0, y_1, \ldots, y_{m-1} \) and \( y = (y_0, y_1, \ldots, y_{m-1}) \) where \( 0 \leq p_0 < p_1 < \cdots < p_{k-1} < m \). Let \( c = (c_0c_1 \cdots c_{k-1}) \) be a binary word of length \( k \), i.e., \( c_i \in \{0,1\} \). Then the vector \( f|_{y=c} \) is defined to be the complex-valued vector with component \( i = \sum_{j=0}^{m-1} i_j 2^j \) equal to \( \omega^{f_{i_0,i_1,\ldots,i_{m-1}}} \) if \( i_{c_j} = c_j \) for each \( 0 \leq c_j < k \) and equal to 0 otherwise. As in the case of \( y \) and \( c \) are all binary vectors. Then, \( f|_{y=c} \) represents the complex-valued vector associated with \( f \).

**Lemma 1 ([29]):** Let \( f, g : A \subseteq \{0,1\}^m \to \mathbb{Z}_q \) be GBFs in variables \( y_0, y_1, \ldots, y_{m-1} \). Let \( y = (y_0, y_1, \ldots, y_{m-1}) \) where \( 0 \leq p_0 < p_1 < \cdots < p_{k-1} < m \) and \( c = (c_0c_1 \cdots c_{k-1}) \) be a binary word of length \( k \), then the function \( f|_{y=c} \) denotes \( z = (z_0z_1 \cdots z_{l-1}) \) where \( 0 \leq i_1 < i_2 < \cdots < i_{k-1} < m \) is a set of indices not in \( \{p_0, p_1, \cdots, p_{k-1}\} \), then for a binary vector \( n = (n_0n_1 \cdots n_{k-1}) \), the following equality holds

\[
C \left(f|_{y=c} \right) \left(g|_{y=n} \right) = \sum_{c_1, c_2} C \left(f|_{y=c_1} \right) \left(g|_{y=c_2} \right),
\]

**Lemma 2 ([21]):** Let \( f : A \subseteq \{0,1\}^m \to \mathbb{Z}_q \) be a GBF in variables \( y_0, y_1, \cdots, y_{m-1} \). Let \( y \) and \( c \) be as defined in Lemma 1, then AACF is given by

\[
A(f) = \sum_{c} A \left(f|_{y=c} \right) + \sum_{c_1 \neq c_2} C \left(f|_{y=c_1} \right) \left(f|_{y=c_2} \right).
\]

**III. PROPOSED CONSTRUCTION OF GCPs**

In this section, we provide a GBFs based construction of GCPs for non-power of two lengths. Unless otherwise stated, this section and subsequent sections assume \( m \geq 5 \).

Suppose \( Q : \{0,1\}^m \to \mathbb{Z}_q \) is the quadratic form in variables \( z_0, z_1, \ldots, z_{m-5} \).

\[
Q(z_0, z_1, \ldots, z_{m-5}) = \sum_{0 \leq i < j < m-4} q_{ij} z_i z_j.
\]

For any \( c_i \in \mathbb{Z}_q \), we define a GBF

\[
f_1 = Q + \sum_{i=0}^{m-5} c_i z_i + c.
\]

Using the notation \( z_i = 1 - z_i \) and \( f_1 \) defined in (9), the proposed GBF \( f : A \to \mathbb{Z}_q \) is defined as

\[
f = f_1 + \frac{q}{2} z_{m-1} (z_{m-4} + z_{m-2} z_{m-3}) + \frac{q}{2} z_1 (z_{m-1} - z_{m-2} z_{m-3} z_{m-4} + z_{m-2} z_{m-3} z_{m-5}) + z_{m-1} z_{m-2} z_{m-3} - 1 \}
\]

where \( A = \{0_m, 1_m, \ldots, 2^{m-1} + 2^{m-3} - 1\} \).

We shall first prove a special case when the quadratic part of \( f \) given in (10) is zero.

**Lemma 3:** Let the quadratic part \( Q \) of \( f|_{x=e} \) is identically equal to zero and \( G(Q|_{x=c}) \) has a single vertex labeled \( \beta \), where \( z = (z_0, z_1, \ldots, z_{m-5}) \) and \( c = (c_0c_1 \cdots c_{m-6}) \) length binary vector. Then

\[
\left(f|_{x=e}, \left(f + \frac{q}{2} \beta + c \right) \right|_{x=e},
\]

forms a GCP of length \( 2^{m-1} + 2^{m-3} \), with exactly 20 non-zero elements.

**Proof:** Since \( f_1|_{x=e} \) is a function containing only one variable \( z_\beta \), so \( f_1|_{x=e} \) gives exactly 2 non-zero elements in the sequence. The binary variables \( z_{m-4}, z_{m-3}, z_{m-2} \) and \( z_{m-1} \) remain unaffected by \( z = c \), and since the length of the sequence is \( 10 \times 2^{m-4} \), so the function \( f|_{x=e} \) takes non-zero values in exactly 20 components numbered \( k2^{m-4} + \sum_{j \neq \beta} c_j 2^j \), \( 0 \leq k \leq 9 \) and \( \beta^2 + k2^{m-4} + \sum_{j \neq \beta} c_j 2^j \), \( 0 \leq k \leq 9 \). These non-zero terms are placed in increasing order as follows

\[
\{\omega^\gamma, \omega^\delta, \omega^\gamma, \omega^\delta, -\omega^\gamma, -\omega^\delta, \omega^\gamma, \omega^\delta, -\omega^\gamma, -\omega^\delta\},
\]

where \( \gamma \) and \( \delta \) are the values taken by the function \( f_1|_{x=e} \) at \( \sum_{j \neq \beta} c_j 2^j \) and \( 2^\beta + \sum_{j \neq \beta} c_j 2^j \) respectively.
The function \( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e} \) takes values \( \gamma + c' \) and \( \delta + \frac{q}{2} + c' \) at positions \( \sum_{j \neq \beta} c_j 2^j \) and \( 2^j + \sum_{j \neq \beta} c_j 2^j \) respectively. So the 20 non-zero components of the function \( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e} \) at positions mentioned above are placed in increasing order as follows

\[
\{ \omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, \omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'}, -\omega^{\gamma+c'}, -\omega^{\delta+c'} \}.
\]

The non-zero value of the AACS of the vectors corresponding to \( f \mid_{z=e} \) and \( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e} \) occurs only at shifts \( s = k 2^{m-4} + 2^\delta, 0 \leq k \leq 9 \) and \( s = k 2^{m-4} - 2^\delta, 1 \leq k \leq 9 \). For \( s = k 2^{m-4} + 2^\delta \) and \( 0 \leq k \leq 9 \), the AACS of the above two functions are expressed as

\[ A(f \mid_{z=e}) (s) = t_k \omega^{\gamma - \delta}, \tag{12} \]

and

\[ A \left( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e} \right) (s) = t_k \omega^{\gamma + c'} (-\omega^{\delta + c'})^*, \tag{13} \]

where \( t_k \) is some constant.

Similarly for \( s = k 2^{m-4} - 2^\delta \) and \( 1 \leq k \leq 9 \), the above can be written as

\[ A(f \mid_{z=e}) (s) = t_k \omega^{\gamma + \delta}, \tag{14} \]

and

\[ A \left( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e} \right) (s) = t_k (-\omega^{\gamma + c'}) (-\omega^{\delta + c'})^*, \tag{15} \]

where \( t_k \) is some constant. So the AACS is zero for all \( s \neq 0 \), and hence the result follows.

Some notations are defined below for proving the general case of construction of GCPs of non-power of two length. Let \( 0 \leq p_0 < p_1 < \cdots < p_{k-1} < m - 4 \), be a list of \( k \) indices, where \( 0 \leq k \leq m - 5 \) and \( z = (z_{p_0}, z_{p_1}, \ldots, z_{p_{k-1}}) \). Let the remaining \( m - 4 - k \) indices between 0 to \( m - 5 \) be \( 0 \leq i_0 < i_1 < \cdots < i_{k-1} < m - 4 \). Let \( e = (c_0 c_1 \cdots c_{k-1}) \) be a \( k \) length binary vector.

**Theorem 1:** Let us consider the restricted function \( f \mid_{z=e} \) that is obtained by restricting the variables \( z_{p_0}, 0 \leq \alpha \leq k \leq m - 5, \) of GBF \( f \) in (10) with the property that \( G(Q \mid_{z=e}) \) is a path. Let \( \beta_1 \) and \( \beta_2 \) be the two end vertices of the path \( G(Q \mid_{z=e}) \) when \( 0 \leq k \leq m - 5 \). In case of \( k = m - 5 \), \( G(Q \mid_{z=e}) \) has only a single vertex labeled \( \beta = \beta_1 = \beta_2 \). Then for any \( c' \in Z_q \), the complex-valued vectors \( f \mid_{z=e} \) and \( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e} \) forms a GCP of length \( 2^{m-1} + 2^{m-3} \).

**Proof:** We prove the result using induction on \( k \), where the statement of the theorem is taken as an inductive hypothesis. The case when \( k = m - 5 \), follows directly from Lemma 3. Now, let the theorem be true when \( k \) contains \( k + 1 \) variables, and we consider the case for \( k \) variables, where \( 0 \leq k < m - 5 \). When \( G(Q \mid_{z=e}) \) is a path, the non-zero components of function \( f \) are determined by the values of function \( f \mid_{z=e} \) in variables \( (z_{i_0}, z_{i_1}, \ldots, z_{i_{m-k-5}}, z_{m-4}, z_{m-3}, z_{m-2}, z_{m-1}) \).

So for some permutation \( \pi \) of \( \{0, 1, \ldots, m - k - 5\} \) and \( c_0, c_1, \ldots, c_{m-k-5}, c \in Z_q, \) we get the function

\[ f \mid_{z=e} (z_{i_0}, z_{i_1}, \ldots, z_{i_{m-k-5}}, z_{m-4}, z_{m-3}, z_{m-2}, z_{m-1}) = \frac{q}{2} \sum_{\alpha=0}^{m-k-5} z_{\pi(\alpha)} z_{\pi(\alpha+1)} + \sum_{\alpha=0}^{m-k-5} c_\alpha z_{\pi(\alpha)} + c \]

\[ + \frac{q}{2} z_{\pi(m-k-5)} (z_{m-1} z_{m-2} z_{m-3} z_{m-4} + z_{m-2} z_{m-3}) + z_{m-1} z_{m-2} z_{m-3} \]  \hspace{1cm} (16)

The higher order terms in (16) is utilized frequently, so for simplicity, it is denoted by \( R \) as follows

\[ R = \frac{q}{2} z_{\pi(m-k-5)} (z_{m-1} z_{m-2} z_{m-3} z_{m-4} + z_{m-2} z_{m-3}) + z_{m-1} z_{m-2} z_{m-3} \]  \hspace{1cm} (17)

Now, the aim is to prove that the sequences \( f \mid_{z=e} \) and \( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e}, \) where \( c' \in Z_q \), forms a GCP of length \( 2^{m-1} + 2^{m-3} \). If \( s \neq 0 \) is chosen arbitrarily, then the sum of AACS of the sequences is given by

\[ A(f \mid_{z=e}) (s) + A \left( \left( f + \frac{q}{2} z_\beta + c' \right) \mid_{z=e} \right) (s) = A(g_1(s)) + A(g_2(s)) \]  

\[ + A(g_3(s)) + A(g_4(s)) + A(g_5(s)) + A(g_6(s)) + A(g_7(s)). \]  \hspace{1cm} (18)

where \( g_1 = f \mid_{z=e} (z_{\pi(0)}, z_{\pi(1)}, \ldots, z_{\pi(m-k-5)}, z_{m-4}, z_{m-3}, z_{m-2}, z_{m-1}) \) and \( g_2 = f \mid_{z=e} (z_{\pi(0)}, z_{\pi(1)}, \ldots, z_{\pi(m-k-5)}, z_{m-4}, z_{m-3}, z_{m-2}, z_{m-1}). \)  \hspace{1cm} (19)

While for \( k = m - 6 \), it is given by

\[ h_1 (z_{\pi(0)}, z_{\pi(1)}, \ldots, z_{\pi(m-k-5)}, z_{m-4}, z_{m-3}, z_{m-2}, z_{m-1}) = c_1 z_{\pi(1)} + c + R. \]  \hspace{1cm} (20)

Similarly, by substituting \( z_{\pi(0)} = 0 \) in the function \( f \mid_{z=e} \), function \( h_2 \) is obtained which yields the non-zero components of the vector \( g_2 \). The function \( h_2 \) is given by

\[ h_2 (z_{\pi(0)}, z_{\pi(1)}, \ldots, z_{\pi(m-k-5)}, z_{m-4}, z_{m-3}, z_{m-2}, z_{m-1}) = h_1 + z_{\pi(1)} + c_0. \]  \hspace{1cm} (21)

To easily calculate the AACS of \( g_2 \), we consider the vector \( g_2' \) as

\[ g_2' = \left( f + \frac{q}{2} z_{\pi(1)} + c_0 \right) \mid_{z=e} = 0. \]  \hspace{1cm} (22)

Substituting \( z = e \) and \( z_{\pi(0)} = 0 \) in (22) the function \( h_1 + \frac{q}{2} z_{\pi(1)} + c_0 \) is obtained which is identical to \( h_2 \). In component \( i \), the value of the vector \( g_2 \) is the same as the value of the vector \( g_2' \) in the position \( i - \frac{q}{2} z_{\pi(1)} \) (i.e., in non-zero positions,
\(g_2\) is simply a shift of \(g'_2\). Therefore, the vectors \(g_2\) and \(g'_2\) have identical AACFs. Now, consider the pair

\[
g_1 = f|_{z_i=0} = c_0,
\]

and

\[
g'_2 = \left(f + \frac{g}{2} z_i + c_0\right)|_{z_i=0} = c_0.
\]

From the above, it is observed that \(g_1\) corresponds to a GFB \(h_1\) such that the graph of the quadratic part of \(h_1\) is a path on \(m - k - 5\) vertices. Additionally, either \(i_{r(1)}\) is an end vertex of this path, or \(k = m - 6\) and it is the single vertex in the graph. By the inductive hypothesis, \(g_1\) and \(g'_2\) forms a GCP, hence for \(s \neq 0\), the sum of AACF of \(g_1\) and \(g'_2\) is

\[
\mathcal{A}(g_1)(s) + \mathcal{A}(g'_2)(s) = 0.
\]

Since, \(\mathcal{A}(g_2)(s) = \mathcal{A}(g'_2)(s)\) for every s, the sum of AACF \(g_1\) and \(g'_2\) is expressed as

\[
\mathcal{A}(g_1)(s) + \mathcal{A}(g'_2)(s) = 0.
\]

By substituting \(z_0 = 0\) (deleting vertices \(z_0, z_1\)), we get \(G(Q)|_{z_0z_1=0}\) is a path. So by Theorem 1, \(f|_{z_0z_1=0}\) and \((f + z_1 + 1)|_{z_0z_1=0}\) forms a GCP of length 160, which is not the form of \(2^m\).

IV. PROPOSED CONSTRUCTION OF MOCSs

In this section, we have proposed a direct construction of \(2^k\) CSs of length \(2^{m-1} + 2^{m-3}\) with the property that any two CSs are mutually orthogonal to each other.

Let \(Q\) and \(f\) be defined in (8) and (10) respectively \((q = 2)\). For \(0 \leq t < 2^k\), \(0 \leq k \leq m - 5\), the ordered set \(S_t\) (with the natural order induced by the binary vector \((a_0 a_1 \cdots a_{k-1})\)) is defined as

\[
S_t = \left\{ f + \sum_{n=0}^{k-1} a_n z_{p_n} + \sum_{n=0}^{k-1} n_a z_{p_n} + a z_{\beta_2} : a, a_n \in \{0, 1\} \right\},
\]

where \(t = \sum_{n=0}^{k-1} a_n 2^n\). "\(1\)" represents a vector all of whose component is one and \(\oplus\) denotes addition modulo 2.

Theorem 2: Suppose that \(G(Q)\) contains a set of \(k \leq m - 5\) distinct vertices labeled \(p_0, p_1, \ldots, p_{k-1}\) with the property that deleting those \(k\) vertices and all their edges results in a path. Let \(\beta_1\) and \(\beta_2\) be the two end vertices of the path. In case of single vertex let \(\beta_1 = \beta_2 = \beta\). Then for any \(0 \leq t < 2^k\), the set \(S_t\) is a CS. Also for the case \(t' \neq t\), the sets \(S_{t'}\) and \(S_t\) are MOCSs.

Proof: Since each \(S_t\) for \(1 \leq t < 2^k\) is a permutation of \(S_0\), so proving \(S_0\) is a complementary set is sufficient to show that for any \(0 \leq t < 2^k\), the set \(S_t\) is a CS.

Let \(z = (z_{p_0}, z_{p_1}, \ldots, z_{p_{k-1}})\) and \(a = (a_0 a_1 \cdots a_{k-1})\). So \(\mathbf{a} \cdot z = \sum_{n=0}^{k-1} a_n z_{p_n}\). Now from Lemma 2, for \(s \neq 0\), sum of AACF can be expressed as

\[
\sum_{\mathbf{a}} S_{1} = \sum_{\mathbf{a}} A((f + \mathbf{a} \cdot z + a z_{\beta_2})(s)) = L_1 + L_2,
\]

where

\[
L_1 = \sum_{\mathbf{a}} A((f + \mathbf{a} \cdot z + z_{\beta_2})(s)),
\]

and

\[
L_2 = \sum_{\mathbf{c}, \mathbf{c} \neq \mathbf{e}} \sum_{\mathbf{a}} A((f + \mathbf{a} \cdot z + a z_{\beta_2})(s))
\]

The graph \(G(Q)\) (quadratic part of \(f\)) is given in Fig. 1.

![Fig. 1: The graph of quadratic part \(Q\) of \(f\)](image)
Now, the vector $z$ contains all the terms of $a \cdot z$. So for the fixed values of $c_1, c_2$ and $a$, we have,

$$ (f + a \cdot z + az_{\beta_2}) |_{z = e_1} = \begin{cases} 
    e_1 = (f + az_{\beta_2}) |_{z = e_1}, & \text{when } a \cdot c_1 = 0 \pmod{2}, \\
    -e_1, & \text{when } a \cdot c_1 = 1 \pmod{2}.
\end{cases} $$

Therefore for the fixed values of $c_1, c_2$ and $a$, from (35) and (36) ACCF values are obtained as

$$ C \left( (f + a \cdot z + az_{\beta_2}) |_{z = e_1}, (f + a \cdot z + az_{\beta_2}) |_{z = e_2} \right) (s) \begin{cases} 
    C(e_1, e_2), & \text{when } a \cdot c_1 = a \cdot c_2 = 0 \pmod{2}, \\
    C(-e_1, -e_2), & \text{when } a \cdot c_1 = a \cdot c_2 = 1 \pmod{2}, \\
    C(e_1, -e_2), & \text{when } a \cdot c_1 = 0 \pmod{2}, a \cdot c_2 = 1 \pmod{2}, \\
    C(-e_1, e_2), & \text{when } a \cdot c_1 = 1 \pmod{2}, a \cdot c_2 = 0 \pmod{2}.
\end{cases} $$

(36)

Since, $C(e_1, e_2) = C(-e_1, -e_2)$ and $C(e_1, -e_2) = C(-e_1, e_2)$, the above can be re-expressed as

$$ C \left( (f + a \cdot z + az_{\beta_2}) |_{z = e_1}, (f + a \cdot z + az_{\beta_2}) |_{z = e_2} \right) (s) \begin{cases} 
    C(e_1, e_2)(s), & \text{when } a \cdot c_1 = a \cdot c_2 \pmod{2}, \\
    C(e_1, -e_2)(s), & \text{when } a \cdot c_1 = 1 \pmod{2}.
\end{cases} $$

(37)

(38)

Due to the fact that $c_1 \neq c_2$, $c_1 + c_2 \neq 0 \pmod{2}$, and so the linear functional $a \cdot (c_1 + c_2) \pmod{2}$ takes each value $0$ and $1$ precisely $2^{k-1}$ times, i.e., an equal number of times. So, from (39) the inner sum of $L_2$ is zero and so is $L_2$. Hence it is proved that $S_t$ is a CS of size $2^k$.

Now, let $n = (n_0n_1 \cdots n_{k-1})$, $t = \sum_{a=0}^{k-1} n_a 2^a$ and $t' = \sum_{a=0}^{k-1} n'_a 2^a$. It needs to prove that for $t \neq t'$, $S_t$ and $S_{t'}$ are mutually orthogonal. From Lemma 1, the sum of ACCF can be written as

$$ \sum_{a,n} C \left( (f + a \cdot n) \cdot z + az_{\beta_2}, f + (a + n') \cdot z + az_{\beta_2} \right) (s) = M_1 + M_2, $$

(40)

where

$$ M_1 = \sum_{a,n} \sum_{c_1 \neq c_2} C \left( (f + a \cdot n) \cdot z + az_{\beta_2}, f + (a + n') \cdot z + az_{\beta_2} \right) |_{z = e_1}, $$

(41)

and

$$ M_2 = \sum_{a,n} \sum_{c} C \left( (f + a \cdot n) \cdot z + az_{\beta_2}, f + (a + n') \cdot z + az_{\beta_2} \right) |_{z = e_2}, $$

(42)

For the fixed $c_1, c_2$ and $a$, we consider the following sum of $M_1$

$$ \sum_{a} C \left( (f + a \cdot n) \cdot z + az_{\beta_2}, f + (a + n') \cdot z + az_{\beta_2} \right) |_{z = e_1} = M_1 \cdot (f + (a + n') \cdot z + az_{\beta_2}) |_{z = e_1}, $$

$$ (f + (a + n') \cdot z + az_{\beta_2}) |_{z = e_2} = \sum_{a} C \left( (f + (a + n) \cdot z + az_{\beta_2}) |_{z = e_1}, (f + (a + n') \cdot z + az_{\beta_2}) |_{z = e_2} \right) (s) = \sum_{a} \left( -1 \right)^{n \cdot (c_1 \oplus c_2)} C \left( (f + n \cdot z + az_{\beta_2}) |_{z = e_1}, (f + n' \cdot z + az_{\beta_2}) |_{z = e_2} \right) (s) = C \left( (f + n \cdot z + az_{\beta_2}) |_{z = e_1}, (f + n' \cdot z + az_{\beta_2}) |_{z = e_2} \right) (s) \sum_{a} \left( -1 \right)^{n \cdot (c_1 \oplus c_2)}. $$

(43)

Since $c_1 \neq c_2$, so the function $a \cdot (c_1 + c_2)$ in (43) takes values $0$ and $1$ equal number of times and hence (43) vanishes for all $s$.

Now for the fixed $a$ and $c$ consider the following sum of $M_2$

$$ \sum_{a} C \left( (f + a \cdot n) \cdot z + az_{\beta_2}, f + (a + n') \cdot z + az_{\beta_2} \right) |_{z = e_1}, $$

$$ (f + (a + n') \cdot z + az_{\beta_2}) |_{z = e_2} = \sum_{a} C \left( (f + a \cdot n) \cdot c + az_{\beta_2}, (f + a + n') \cdot c + az_{\beta_2} \right) |_{z = e_2} = \sum_{a} C \left( (f + (n + n') \cdot c + az_{\beta_2}) |_{z = e_1}, (f + (a + n') \cdot c + az_{\beta_2}) |_{z = e_2} \right) (s) = (-1)^{(n \oplus n') \cdot c} \sum_{a} C \left( (f + az_{\beta_2}) |_{z = e_1}, (f + az_{\beta_2}) |_{z = e_2} \right) (s) = (-1)^{(n \oplus n') \cdot c} A \left( f |_{z = e_1} \right) (s) + A \left( f + az_{\beta_2} \right) |_{z = e_2} (s). $$

(44)

From Theorem 1, the above sum in (44) is zero for all $s \neq 0$. For $s = 0$, ACCF is

$$ \sum_{a,n} C \left( (f + (n + n') \cdot c + az_{\beta_2}) |_{z = e_1}, (f + az_{\beta_2}) |_{z = e_2} \right) (s) = \sum_{a} C \left( (f + (n + n') \cdot c + az_{\beta_2}) |_{z = e_1}, (f + az_{\beta_2}) |_{z = e_2} \right) (s) = (-1)^{(n \oplus n') \cdot c} \cdot 2^{m-k-4}. $$

(45)

For $c \in \mathbb{Z}_k^2$, substituting this back in (44), we get the sum of ACCF as

$$ \sum_{a} C \left( (f + (n + n') \cdot c + az_{\beta_2}) |_{z = e_1}, (f + az_{\beta_2}) |_{z = e_2} \right) (s) = (-1)^{(n \oplus n') \cdot c} \cdot 2^{m-k-3}. $$

(46)

Here $t \neq t'$ is considered, which implies $n \neq n'$, and hence $n \oplus n' \neq 0$. So the linear functional $(n \oplus n') \cdot c$ (regarded as a function of $c$) is not equivalent to the zero function. As a result, it is balanced, i.e., the values $0$ and $1$ are taken equal number of times by the function as $c$ varies. Hence the sum

$$ \sum_{c} (-1)^{(n \oplus n') \cdot c} \cdot 2^{m-k+1} = 0. $$

(47)

**Remark 1:** [23, Th. 4] generates CSs of length $2^{m-1} + 2^{m-3}$ and set size for $\nu = m - 3$, which is covered by Theorem 2 of our proposed construction by taking $k = 2$.

**Remark 2:** By taking $\nu = m - 3$, [24, Th. 4] and $t = m - 3$, [27, Th. 3] generates CSs of length $2^{m-1} + 2^{m-3}$ and set size $2^{k+1}$. The proposed construction of CSs in Theorem 2 covers these special cases of [23], [27].
TABLE I: Comparison of the proposed MOCS construction with the existing direct constructions of [44], [45]

| Ref. | Parameters | Based on | Length(N) | Constraint |
|------|------------|----------|----------|-----------|
| [44] | $(2^m, 2^{3^2}, N)$ | GBF of order 2 | $2^{m-1} + 2^t$ | $m \leq t \leq m \leq n \leq m$ |
| [55] | $(2^{m+1}, 2^{3^2}, N)$ | GBF of order 2 | $2^m + 2^t$ | $m \leq t \leq m \leq n \leq m$ |
| Theorem 2 | $(2^{m+1}, 2^{3^2}, N)$ | GBF of order $2^m - 2^t, 2^m - 2^t, 2^m - 2^t$ | $m \geq 3$ |

TABLE I compares the proposed constructions of MOCSs with the existing direct constructions of [44], [45].

Example 3: Let us consider the same GBF as given in Example 2, and the deleted vertices are also same, i.e., $z_0, z_3$. Then the set,

\[ S_0 = \{ f, f + z_1, f + z_0, f + z_0 + z_1, f + z_3, f + z_3 + z_1, f + z_3 + z_0, f + z_3 + z_1 + z_0 \}, \]  

(48)

is a CS of size 8 and sequence length 160, which is not of the form of $2^m$. Similarly the sets $S_t$ for $0 \leq t < 4$, which are the permutations of the set $S_0$, are also CS of size 8, with the property that any two different CSs are mutually orthogonal to each other.

V. PROPOSED CONSTRUCTION OF CCCs

In this section first we construct a mate of the MOCSs proposed in section IV. Then binary CCCs of length $2^{m-1} + 2^{m-3}$ are constructed by union of these two MOCSs through GBFs. For a given GBF $f$ in (10), GBF $\tilde{f}: B \rightarrow 2^2$ is defined as

\[ \tilde{f}(z_0, z_1, \ldots, z_{m-1}) = f(z_0, z_1, \ldots, z_{m-1}), \]  

(49)

where $B = \{0, 1\}^m \setminus \{0_m, 1_m, \ldots, (2^{m-2} + 2^{m-3} - 1)_m\}$.

Lemma 4: Let us assume a set of $k \leq m - 5$ distinct vertices labelled with the property that deleting that set of vertices and all the edges transform $G(Q)$ into a path. Let $\beta_1$ and $\beta_2$ be the two end vertices of this path. In case of $k = m - 5$, the single vertex of the graph is denoted by $\beta_1 = \beta_2 = \beta$. Then for each $0 \leq t < 2^k$, the ordered set $S_t$ given by

\[ \left\{ \tilde{f} + \sum_{a=0}^{k-1} a_0 \tilde{z}_{a_0} \tilde{p}_a + \sum_{a=0}^{k-1} a_0 \tilde{z}_{a_0} \tilde{p}_a + \alpha z_{\beta_2} : a, a_0 \in \{0, 1\} \right\}, \]  

(50)

is a CS of size $2^{k+1}$, where $\tilde{f}$ is defined in (49). Further, for $t' \neq t$, $S_{t'}$ and $S_t$ are MOCSs, where the natural order is induced from the binary vector $(aa_0a_1 \cdots a_{k-1})$.

The next theorem gives CCCs of length $2^{m-1} + 2^{m-3}$.

Theorem 3: Let the sets $S_t$ and $\tilde{S}_t$ be defined in Theorem 2 and Lemma 4 respectively, then

\[ \{ S_t : 0 \leq t < 2^k \} \cup \{ \tilde{S}_t : 0 \leq t < 2^k \}, \]  

(51)

forms a $(2^{k+1}, 2^{k+1}, 2^{m-1} + 2^{m-3})$-CCC.

\textbf{Proof:} It will be shown that CSs $S_t$ and $\tilde{S}_t$ are mutually orthogonal to each other. The sum of ACCF of these CSs can be expressed as

\[ \sum_a C (f + (a + n) \cdot z + z_{\beta_2}, \tilde{f} + (a + n') \cdot \tilde{z}) (s) \]

+ $C (f + (a + n) \cdot z, \tilde{f} + (a + n') \cdot \tilde{z} + z_{\beta_2}) (s)$

= \[ \sum_a C \left( (f + (a + n) \cdot z + z_{\beta_2})  \mid z = e_1 \right), \]

\[ (\tilde{f} + (a + n') \cdot \tilde{z})  \mid z = e_2 \) (s)

+ $C \left( (f + (a + n) \cdot z)  \mid z = e_1 \right), \]

\[ (\tilde{f} + (a + n') \cdot \tilde{z} + z_{\beta_2})  \mid z = e_2 \) (s) = M(say)

(52)

For a given $c_1$ and $c_2$, consider the following sum of the first term in (52)

\[ \sum_a C \left( (f + (a + n) \cdot z + z_{\beta_2})  \mid z = e_1 \right), \]

\[ (\tilde{f} + (a + n') \cdot \tilde{z})  \mid z = e_2 \) (s)

= \[ \sum_a C \left( (f + (a + n) \cdot z + z_{\beta_2})  \mid z = e_1 \right), \]

\[ (\tilde{f} + (a + n') \cdot (1 - z))  \mid z = e_2 \) (s)

= \[ C \left( (f + z_{\beta_2})  \mid z = e_1, (\tilde{f} + z_{e_2})  \mid z = e_2 \right) (s) \]

\[ \cdot \sum_a \left( (-1)^{n_1 \oplus n_2} - (-1)^{a \oplus n_1 \oplus n_2} \cdot (-1)^{a_1 \oplus e_1 \oplus e_2} \right) \]

\[ = C \left( (f + z_{\beta_2})  \mid z = e_1, (\tilde{f} + z_{e_2})  \mid z = e_2 \right) (s) \]

\[ \cdot (-1)^{n_1 \oplus n_2} \cdot (-1)^{a_1 \oplus e_1 \oplus e_2} \sum_a \left( (-1)^{a_1 \oplus e_1 \oplus e_2} \right) \]

(53)

The above sum in (53) vanishes whenever $(c_1 \oplus c_2) \neq 1$. So, the first correlation term in (52) is zero whenever $c_1$ and $c_2$ are equal. Thus, summing (53) over all $c_1 \neq c_2$, the above term further can be simplified as

\[ \sum_{e_1 \oplus e_2 = 1} C \left( (f + z_{\beta_2})  \mid z = e_1, (\tilde{f} + z_{e_2})  \mid z = e_2 \right) (s) \]

\[ \cdot (-1)^{n_1 \oplus n_2} \cdot (-1)^{a_1 \oplus e_1 \oplus e_2} \]

\[ = \sum_e C \left( (f + z_{\beta_2})  \mid z = e, (\tilde{f} + z_{e_1 \oplus e_2})  \mid z = e_1 \right) (s) \]

\[ 
\cdot (-1)^{n_1 \oplus n_2} \cdot (-1)^{a_1 \oplus e_1 \oplus e_2} \]

(54)

From Lemma 1, the inner sum of (54) can be further simplified as

\[ C \left( (f + z_{\beta_2})  \mid z = e, (\tilde{f} + z_{e_1 \oplus e_2})  \mid z = e_1 \right) (s) \]

\[ + C \left( (f + z_{\beta_2})  \mid z = e_1, (\tilde{f} + z_{e_2})  \mid z = e_2 \right) (s) \]

\[ + C \left( (f + z_{\beta_2})  \mid z = e_2, (\tilde{f} + z_{e_1})  \mid z = e_1 \right) (s) \]

\[ + C \left( (f + z_{\beta_2})  \mid z = e_1, (\tilde{f} + z_{e_2})  \mid z = e_2 \right) (s) \]

(55)
The functions obtained by substituting \( \bar{\text{complex vectors}} \) without loss of generality let

\[
\begin{align*}
&\text{C} \left( f \big|_{\bar{z}_2 = c_0}, \bar{f} \big|_{\bar{z}_2 = \beta_1} \right) (s) \\
&+ \text{C} \left( f \big|_{\bar{z}_2 = c_0}, \bar{f} \big|_{\bar{z}_2 = \beta_1} \right) (s) \\
&- \text{C} \left( f \big|_{\bar{z}_2 = \beta_1}, \bar{f} \big|_{\bar{z}_2 = \beta_1} \right) (s) \\
&- \text{C} \left( f \big|_{\bar{z}_2 = \beta_1}, \bar{f} \big|_{\bar{z}_2 = \beta_1} \right) (s).
\end{align*}
\]

(55)

Similarly, the second term of the correlation in (52) becomes

\[
\sum_{\bar{z}} \text{C} \left( \left( f + (d + n) \cdot z \right) \big|_{\bar{z} = c_1} \right) (s) = \sum_{\bar{e}} \text{C} \left( \left( f + \beta \right) \big|_{\bar{z} = c_1} \right) (s) + \left( -1 \right)^{n \oplus n} c.
\]

(56)

The inner sum of (56) can be simplified as

\[
\begin{align*}
&\text{C} \left( f \big|_{\bar{z} = c_1}, \left( f + \beta \right) \big|_{\bar{z} = c_1} \right) (s) \\
&= \text{C} \left( f \big|_{\bar{z} = c_1}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s) \\
&- \text{C} \left( f \big|_{\bar{z} = \beta_1}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s) \\
&+ \text{C} \left( f \big|_{\bar{z} = \beta_1}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s) \\
&- \text{C} \left( f \big|_{\bar{z} = \beta_1}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s).
\end{align*}
\]

(57)

So from (54), (55), (56) and (57) we get the value of \( M \) in (52) as

\[
\begin{align*}
M &= 2 \sum_{c} \text{C} \left( f \big|_{\bar{z} = c_1}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s) \\
&- \text{C} \left( f \big|_{\bar{z} = \beta_1}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s) = 2^k \cdot \left( -1 \right)^{n \oplus n} c.
\end{align*}
\]

(58)

Since \( G(QI)_{\bar{z} = c} \) is a path, so for some permutation \( \pi \) of \( \{0, 1, \ldots, m - k - 5\} \) and \( c_\alpha, c \in \mathbb{Z}_q \) the function \( f \big|_{\bar{z} = c} \) obtained by substituting \( z = c \) in \( f \) should be of the form

\[
\begin{align*}
f \big|_{\bar{z} = c} &= \sum_{\alpha = 0}^{m-k-5} \pi(\alpha) \pi(\alpha+1) + \sum_{\alpha=0}^{m-k-5} c_\alpha \pi(\alpha) + c \\
&+ \sum_{\bar{z} = \bar{z}_1}^m \left( \bar{z} \cdot \bar{z}_1 \right) \sum_{\bar{z} = \bar{z}_2}^m \left( \bar{z} \cdot \bar{z}_2 \right) + \sum_{\bar{z} = \bar{z}_3}^m \left( \bar{z} \cdot \bar{z}_3 \right).
\end{align*}
\]

(59)

Let \( h_1 \) and \( h_2 \) be the function obtained from \( f \) by substituting \( z = c \), \( \beta_1 = 0 \) and \( z = c \), \( \beta_2 = 1 \) respectively. Further without loss of generality let \( \beta_2 = \pi(0) \). Then both the function can be expressed as

\[
\begin{align*}
h_1 &= \sum_{\alpha = 0}^{m-k-6} \pi(\alpha) \pi(\alpha+1) + \sum_{\alpha=0}^{m-k-5} c_\alpha \pi(\alpha) + c + R, \\
&\text{and} \quad h_2 = h_1 + \pi(1) + c_0.
\end{align*}
\]

(60)

The functions \( h_1 \) and \( h_2 \) give non-zero components of the complex vectors \( e_1 = f \big|_{\bar{z} = 0} \) and \( e_2 = f \big|_{\bar{z} = \beta_1} \) respectively. Similarly, \( h_1 \) and \( h_2 \) give the non-zero components of the vector \( f \big|_{\bar{z} = \beta_1} = c_1 \) respectively. For any complex-valued sequences \( e_1 \) and \( e_2 \) the following identity holds

\[
\text{C} \left( e_1, e_2 \right) (s) = \text{C} \left( e_2, e_1 \right) (s).
\]

(62)

Using the above identity, we get,

\[
\begin{align*}
&\text{C} \left( f \big|_{\bar{z} = c_0}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s) \\
&= \text{C} \left( f \big|_{\bar{z} = \beta_1}, \bar{f} \big|_{\bar{z} = \beta_1} \right) (s),
\end{align*}
\]

(63)

which shows that \( M \) in (58) is zero, and hence the result follows from (52).

**Example 4**: Let us consider the set \( S_t \) for \( 0 \leq t \leq 3 \) as defined in **Example 3**. Now for the same GBD defined in **Example 2**, using Lemma 4 construct a MOCS \( \tilde{S}_t \) (0 \leq t < 4) of length 160 as

\[
\{ \tilde{f} + a_0 \tilde{z}_0 + a_1 \tilde{z}_1 + n_0 \tilde{z}_0 + n_1 \tilde{z}_1 + a \tilde{z}_1 : a, a_0, a_1 \in \{0, 1\} \}
\]

(64)

where \( t = n_0 2^0 + n_1 2^1 \). Then from **Theorem 3**

\[
\{ S_t : 0 \leq t < 4 \} \cup \{ \tilde{S}_t : 0 \leq t < 4 \}
\]

(65)

is a \((8, 8, 160)\)-CCC.

In **TABLE II**, the proposed construction CCC is compared with the existing construction CCC on different parameters.

**VI. CONSTRUCTION OF SEQUENCES OF LENGTH**

\( 2^{m-1} + 2^{m-2} + 2^{m-4} \).

In this section, we have extended our proposed construction to provide GCPs, MOCSs and binary CCCs of length \( 2^{m-1} + 2^{m-2} + 2^{m-4} \).

Consider an integer \( m \geq 6 \), for any \( c, c_i \in \mathbb{Z}_q \), we define a function

\[
f_1(z_0, z_1, \ldots, z_{m-6}) = Q + \sum_{i=0}^{m-6} c_i z_i + c,
\]

(66)

where \( Q \) is the quadratic part in variables \( z_0, z_1, \ldots, z_{m-6} \). Now, we define the GBD \( f : A \rightarrow \mathbb{Z}_q \) as

\[
f = f_1 + \frac{q}{2} \sum_{i=0}^{m-6} c_i z_i + \sum_{i=0}^{m-6} c_0 z_0 + \sum_{i=0}^{m-6} c_0 z_i.
\]

(67)

Let \( A = \{0_m, 1_m, \ldots, 2^{m-1} + 2^{m-2} + 2^{m-4} - 1 \} \). Also we define the GBD \( \bar{f} : B \rightarrow \mathbb{Z}_q \) as

\[
\bar{f}(z_0, z_1, \ldots, z_{m-1}) = \bar{f}(z_0, z_1, \ldots, z_{m-1}),
\]

(68)

where \( B = \{0, 1, \ldots, 2^{m-3} + 2^{m-4} -1 \} \) and \( z_i = 1 - z_i \). Now, by replacing the GBD \( f \) used in the above **Theorems**, by the function \( f \) defined in (67), we can generate GCP, CS and CCC of length \( 2^{m-1} + 2^{m-2} + 2^{m-4} \) \((m \geq 6)\), from **Theorem 1, Theorem 2, Theorem 3**, respectively.

**Remark 3**: The direct construction of MOCSs of length \( 2^{m-1} + 2^{m-3} \) are available in [44] \((t = 2^{m-3})\), but MOCSs of lengths \( 2^{m-1} + 2^{m-2} + 2^{m-4} \) \((m \geq 6)\) has never been reported in the literature.
TABLE II: Comparison of the proposed CCC construction with [8], [29]–[32], [46]

| Ref. | Parameters | Phase | Based on | Length(N) | Constraints |
|------|------------|-------|----------|-----------|-------------|
| [8]  | $(2^{k+1}, 2^{k+1}, N)$ | $q > 2$, $q$ is even | GBF of order $2$ | $2^m$ | $m, k \in Z^+$, $m > 1$ |
| [29] | $(2^{k+1}, 2^{k+1}, N)$ | $q > 2$, $q$ is even | GBF of order $2$ | $2^m$ | $m, k \in Z^+$, $m > 1$ |
| [30] | $(2^k, 2^k, N)$ | $q > 2$, $q$ is even | GBF of order $2$ | $2^m$ | $k, m \in Z^+$, $m > 1, k < m$ |
| [31] | $(2^{k+1}, 2^{k+1}, N)$ | $q > 2$, $q$ is even | GBF of order $2$ | $2^m$ | $m, k \in Z^+$, $m > 1, k < m - 1$ |
| [32] | $(2^k, 2^k, N)$ | $q > 2$, $q$ is even | GBF of order $2$ | $2^m$ | $m, k \in Z^+$, $m > 3, 1 < k \leq m$ |
| [46] | $(M, M, N)$ | $q = \text{lcm}(p_1, p_2, \ldots, p_k)$ | MVF of order $2$ | $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ | $r, m_i \in Z^+$, $p_i$ is prime, $1 \leq i \leq k$, |
| Theorem 3 | $(2^{k+1}, 2^{k+1}, N)$ | $2$ | GBF of order $2$ | $2^m + 2^{m-3}$ | $m, k \in Z^+$, $m > 5$ |
|       |            |       |          | $2^m - 2^{m-1} + 2^{m-3} + 2^{m-4}$ | $m, k \in Z^+$, $m > 6$ |

Example 5: For $m = 8$ and $q = 2$, let us consider the GBF $f: \{0_8, 1_8, \ldots, 208_8\} \rightarrow Z_2$ defined as

$f = z_0 z_1 + z_0 z_2 + z_1 z_2 + z_1 (\bar{z}_0 + \bar{z}_1 z_2)$

$+ (z_2 \bar{z}_0 + z_2 z_0 + \bar{z}_2 z_1 + z_2 + \bar{z}_2 z_0 + \bar{z}_2 z_1 + z_2 + \bar{z}_2 z_0 + \bar{z}_2 z_1)$

$+ z_1 \bar{z}_0 + z_1 z_0 + \bar{z}_1 z_2 + z_1 + \bar{z}_1 z_0 + \bar{z}_1 z_1 + z_1 + \bar{z}_1 z_0 + \bar{z}_1 z_1$.

In this example, after deleting vertex $z_2$, $f$ forms a path, so the sets

$S_0 = \{f + a_0 z_2 + a z_0 : a, a_0 \in \{0, 1\}\}$, (70)

and $S_1 = \{f + a_0 z_2 + a z_0 + z_2 : a, a_0 \in \{0, 1\}\}$, (71)

are MOCSs of length 208. Similarly the sets

$\bar{S}_0 = \{f + a_0 z_2 + a z_0 : a, a_0 \in \{0, 1\}\}$, (72)

and $\bar{S}_1 = \{f + a_0 z_2 + a z_0 + z_2 : a, a_0 \in \{0, 1\}\}$, (73)

are MOCSs of length 208 and hence their union i.e., the set

$\{S_0, S_1, \bar{S}_0, \bar{S}_1\}$ forms a $(4, 4, 208)$-CCC.

VII. PMEPR of MOCSs and CCCs

In this section, the row and column sequence PMEPR of the sequences generated by Theorem 2, Theorem 3 and MOCSs and CCCs constructed in the section VI are investigated. The PMEPR of the CCC-MC-CDMA system is determined by the column sequences of the complementary matrices when each complementary code is arranged as a matrix [8]. Thus, in this section, the column sequence PMEPR of constructed MOCSs and CCCs is effectively bounded by 2.

Since the row sequences of $S_i$ forms a CS of size $2^k$, its PMEPR is upper bounded by $2^k$. The column sequence PMEPR of the CCC generated from Theorem 3 can be bounded above by 2 by adding a suitable constant. For GBFs $f, g$ and constants $c_1, c_2$, $c_2$ can be easily verified that $A(f + c) = A(f) + c$, $c_1, c_2 \subset C(f, g)$. For a permutation $\sigma$ of $\{0, 1, \ldots, k - 1\}$, the set (matrix) $S_i$ of (31) is redefined by adding the constant $\sum_{\alpha=0}^{k-1} a_\alpha(\sigma)(\sigma(\alpha)+1)$

$$
\begin{align*}
&\left\{f + \sum_{\alpha=0}^{k-1} a_\alpha z_\alpha + \sum_{\alpha=0}^{k-1} n_\alpha z_\alpha + a z_\beta + \\
&\sum_{\alpha=0}^{k-2} a_\alpha(\sigma)(\sigma(\alpha)+1) : a, a_\alpha \in \{0, 1\}\right\},
\end{align*}
$$

where $t = \sum_{\alpha=0}^{k-1} n_\alpha 2^\alpha$. Adding the same constant to the set $\bar{S}_i$ and noting that AACS remains unchanged and ACCS changes by a constant, so the new set is still a CCC with same parameters. It can be observed it from (74) that the $\ell$th column of $S_i$ can be obtained by fixing $z = (i_0, i_1, \ldots, i_{m-1})$, $0 \leq z < 2^m-1 + 2^m-3$. So $\ell$th column of the matrix $S_i$ is dependent on a function $\phi$ defined as

$$
\phi(a) = \sum_{\alpha=0}^{k-1} a_\alpha(\sigma(a)) a_\alpha(\sigma(a)+1) + \sum_{\alpha=0}^{k-1} a_\alpha i_{p_\alpha} + a z_\beta + C,
$$

where $C$ is a constant (independent of $a$). Since any column sequence of the matrix $S_i$ is obtained by a GBF, whose graph is a path consisting of $k$ vertices. Hence, from [20] the $\ell$th column of $S_i$ is a Golay sequence, and so its PMEPR is upper bounded by 2. Similarly it can be verified that the column sequence PMEPR of $\bar{S}_i$ is also upper bounded by 2. So the maximum column sequence PMEPR of $(2^k, 2^k, 2^m-1 + 2^m-3)$-CCC can be suitably upper bounded by 2. The same is true for $(2^k+1, 2^k+1, 2^m-2 + 2^m-4)$-CCC.

Remark 4: There exist PU matrix based construction of CCCs of length non-power of two [40]–[42], but their column sequence PMEPR are high compared to the proposed construction.

VIII. Conclusion

In this paper, we have proposed a direct and generalized construction of GCP and binary CCC of non-power of two lengths by using higher-order GBFs. The resultant CCCs can be obtained directly from GBFs without using other tedious sequence operations. The non-power of two length binary CCCs directly constructed using GBFs finds many applications in wireless communication due to its simple modulo-2 arithmetic operation, modulation and good correlation properties. Column sequence PMEPR of the proposed CCC can be effectively reduced to be upper bounded by 2. The construction of MOCSs of non-power of two lengths is also provided in this paper. The proposed work solved the open problem cited in [44], [45]. The work is compared with existing literature.

REFERENCES

[1] M. Golay, “Complementary series,” *IRE Trans. Inf. Theory*, vol. 7, no. 2, pp. 82–87, Apr. 1961.
[2] C.-C. Tseng and C. Liu, “Complementary sets of sequences,” *IEEE Trans. Inf. Theory*, vol. 18, no. 5, pp. 644–652, 1972.
[3] H.-H. Chen, S.-W. Chu, and M. Guizani, “On next generation CDMA technologies: The real approach for perfect orthogonal code generation,” *IEEE Trans. Veh. Technol.*, vol. 57, no. 5, pp. 2822–2833, 2008.
[4] N. Suehiro and M. Hatori, “N-shift cross-orthogonal sequences,” *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 143–146, 1988.
[5] S.-M. Tseng and M. Bell, “Asynchronous multicarrier DS-CDMA using mutually orthogonal complementary sets of sequences,” IEEE Trans. Commun., vol. 48, no. 1, pp. 53–59, 2000.

[6] 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.

[7] H. Chen, The Next Generation CDMA Technologies. wiley, Jul. 2007, publisher Copyright: © 2007 John Wiley & Sons Ltd. All Rights Reserved.

[8] Z. Liu, Y. L. Guan, and U. Parampalli, “New complete complementary codes for peak-to-mean power control in multi-carrier CDMA,” IEEE Trans. Commun., vol. 62, no. 3, pp. 1105–1113, 2014.

[9] Z. Liu, Y. L. Guan, and H.-H. Chen, “Fractional-delay-resilient receiver design for interference-free MC-CDMA communications based on complete complementary codes,” IEEE Trans. Wireless Commun., vol. 14, no. 3, pp. 1226–1236, 2015.

[10] S. Wang and A. Adhikary, “MIMO ISI channel estimation using uncorrelated Golay complementary sets of polyphase sequences,” IEEE Trans. Veh. Technol., vol. 56, no. 5, pp. 3024–3039, 2007.

[11] S. Li, J. Chen, and L. Zhang, “Optimisation of complete complementary codes in MIMO radar system,” Electron. Lett., vol. 46, pp. 1157–1159, 2010.

[12] 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.

[13] C.-Y. Chen, Y.-J. Lin, Z.-M. Huang, and C.-Y. Chen, “Z-complementary binary sequences,” in IRE Trans. Info. Theory, vol. 26, no. 2, pp. 1931–1934, 2019.

[14] T. Kojima, T. Tachikawa, A. Ozumi, 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.

[15] M. Golay, “Complementary series,” IRE Trans. Info. Theory, vol. 7, no. 2, pp. 82–87, 1961.

[16] P. Fan, W. Yuan, and Y. Tu, “Z-complementary binary sequences,” IEEE Signal Process. Lett., vol. 14, no. 8, pp. 509–512, Aug. 2007.

[17] B. Shen, Y. Yang, Z. Zhou, P. Fan, and Y. Guan, “New optimal binary Z-complementary pairs of odd length 2m+3,” IEEE Signal Process. Lett., vol. 26, no. 12, pp. 1931–1934, 2019.

[18] C. Xie and Y. Sun, “Constructions of even-period binary Z-complementary pairs with large ZCZs,” IEEE Signal Process. Lett., vol. 25, no. 8, pp. 1141–1145, 2018.

[19] B. Shen, Y. Yang, and Z. Zhou, “A construction of binary Golay complementary sets based on even-shift complementary pairs,” IEE Commun. Lett., vol. 8, pp. 29882–29890, 2020.

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

[21] K. G. Paterson, “Generalized Reed-Muller codes and power control in OFDM modulation,” IEEE Trans. Info. Theory, vol. 46, no. 1, pp. 104–120, Jan. 2000.

[22] R. Turyn, “Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression and surface wave encodings,” J. Combin. Theory (A), vol. 16, pp. 313–333, 1974.

[23] C.-Y. Chen, “Complementary sets of non-power-of-two length for peak-to-average power ratio reduction in OFDM,” IEEE Trans. Inf. Theory, vol. 62, no. 12, pp. 7538–7545, 2016.

[24] ——, “A new construction of golay complementary sets of non-power-of-two length based on Boolean functions,” in IEEE Wirel. Commun. New Conf. (WCNC), 2017, pp. 1–6.

[25] ——, “A novel construction of complementary sets with flexible lengths based on Boolean functions,” IEEE Commun. Lett., vol. 22, no. 2, pp. 260–263, 2018.

[26] A. R. Adhikary and S. Majhi, “New constructions of complementary sets of sequences of lengths non-power-of-two,” IEEE Commun. Lett., vol. 23, no. 7, pp. 1119–1122, 2019.

[27] Y.-J. Lin, Z.-M. Huang, and C.-Y. Chen, “Golay complementary sets and multiple-shift complementary sets with non-power-of-two length and bounded PAPRs,” IEEE Commun. Lett., vol. 25, no. 5, pp. 2805–2809, 2021.

[28] 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.