New Construction of Complementary Sequence (or Array) Sets and Complete Complementary Codes

Zilong Wang\textsuperscript{a}, Member, IEEE, Dongxu Ma\textsuperscript{a}, Guang Gong\textsuperscript{b}, Fellow, IEEE, and Erzhong Xue\textsuperscript{c}

Abstract—A new method to construct $q$-ary complementary sequence sets (CSSs) and complete complementary codes (CCCs) of size $N$ is proposed by using desired para-unitary (PU) matrices. The concept of seed PU matrices is introduced and a systematic approach on how to compute the explicit forms of the functions in constructed CSSs and CCCs from the seed PU matrices is given. A general form of these functions only depends on a basis of the functions from $\mathbb{Z}_N$ to $\mathbb{Z}_4$ and representatives in the equivalent class of Butson-type Hadamard (BH) matrices. Especially, the realization of Golay pairs from our general form exactly coincides with the standard Golay pairs. The realization of ternary complementary sequences of size 3 is first reported here. For the realization of the quaternary complementary sequences of size 4, almost all the sequences derived here are never reported before. Generalized seed PU matrices and the recursive constructions of the desired PU matrices are also studied, and a large number of new constructions of CSSs and CCCs are given accordingly. From the perspective of this paper, all the known results of CSSs and CCCs with explicit GBF form in the literature (except non-standard Golay pairs) are constructed from the WHT matrices. This suggests that the proposed method with other BH matrices will yield a large number of new CSSs and CCCs with the significantly increasing number of the sequences of low peak-to-mean envelope power ratio.

Index Terms—Complementary sequence set, complete complementary codes, Hadamard matrix, Boolean function, PMEPR.

I. INTRODUCTION

GOLAY sequence pair (GSP) was first introduced by Golay in [17] when he studied infrared spectrometry [16]. The concept of GSP was extended later to complementary sequence set (CSS) for binary case [49] and polyphase case [45].

Sequences in GSPs and CSSs have found many applications in physics, combinatorics and telecommunication such as channel measurement, synchronisation and spread spectrum communications. In particular, orthogonal frequency division multiplexing (OFDM) has recently seen rising popularity in international standards including coming 5G cellular systems. However, a major drawback of OFDM is the high peak-to-mean envelope power ratio (PMEPR) of uncoded OFDM signals [31]. Among all the approaches that have been proposed to deal with this power control problem, one of the most attractive methods is coding across the subcarriers and selecting codewords with lower PMEPR. These codewords can be a linear code or codewords drawn from cosets of a linear code [19], [35], [47]. It has been shown in [36] the use of Golay sequences as codewords results in OFDM signals with PMEPR of at most 2.

Golay [17] first proposed two recursive algorithms to construct binary GSPs of length $2^n$. In 1999, Davis and Jedwab’s milestone work [10] showed that the Golay sequences described in [17] can be obtained from specific second-order cosets of the first-order generalized Reed-Muller (GRM) code [28]. This established an effective way of combining the coding approach and the use of Golay sequences. However, the rate of this code suffers a dramatic decline when the length increases. In order to increase the code rate, further cosets of the first order GRM code with a slightly larger PMEPR were also proposed by exhaustive search in [10], Paterson [33], [34] studied general second-order cosets of the first-order GRM code, and showed that the codewords of such a coset lie in CSSs of size $N$, where $N$ is related to the graph associated with the quadratic form of the coset. Schmidt [41], [42] developed a sophisticated theory and proposed constructions of sequences with low PMEPR which were contained in higher-order cosets of the first-order GRM code or in cosets of the other linear code.

Several other CSSs constructions have been given in [6], [44], [54]. These results yield more sequences and provide better upper bounds on the PMEPR than the work in [33], [42]. But it is difficult to use them in a practicable coding scheme for OFDM.

A large volume of works have been done along the line of above methods in the past years. For example, non-standard Golay sequences were studied in [13], [14], [20], the exact value of PMEPR of binary Golay sequences was determined in [51], and GSPs with low PMEPR over QAM constellation were constructed in [8], [21], [23], [40], [48], [50], just to list a few.

The concept of complete mutually orthogonal complementary set (CMOCS) or complete complementary code (CCC) was introduced in [49]. CCC is a source to design zero
correlation zone (ZCZ) sequences, which can be used to eliminate the multiple access interference and multi-path interference in QS-CDMA system. Several important methods to construct ZCZ sequences presented in [11], [22], [37]–[39] are all based on the construction of CCCs. In particular, the constructions of CCCs from GRM codes were proposed in [7], [24], [38].

In the aforementioned constructions, the sequences are directly given by generalized Boolean functions (GBFs), so we refer to it simply as GBF-based constructions in this paper. However, in addition to those GBF-based constructions, there exists another approach based on Hadamard matrices to construct CSSs and CCCs. For instance, the first recursive construction of CSSs and CCCs in [49] was obtained by Hadamard matrices. However, how to obtain the explicit function form of the sequences derived by Hadamard-matrix-based methods constitutes an extremely challenge problem for several decades, so these methods are not as popular as the GBF approaches in the literature. On the other hand, based on the observation on the filter bank theory and the design of GSPs [1], a new method to construct GSPs was proposed in [3] by para-unitary (PU) matrices. Here the word “para-unitary” refers to a unitary matrix with polynomial entries. It has been shown in [3] that this PU-matrix-based construction can explain all the standard Golay sequences in [10] and all known GSPs over QAM constellation in [21], [23]. Moreover, some new GSPs over QAM [2], [3] are also derived from this method. Note that PU matrices are rarely used in the literature because they may not be able to map to q-ary sequences.

In 2016, we [52] proposed a new PU-matrix-based construction to generate q-ary CSSs of size \( N \) and length \( N^m \) where \( N \) and \( m \) are both positive integers. Almost at the same time, Budišin [4] also proposed a PU-matrix-based construction on CSSs and CCCs. These two constructions are similar. However, we have introduced the Butson-type Hadamard (BH) matrices to make the PU-matrix-based construction producing q-ary sequences. Das et al. [9] proposed a construction by applying the BH matrices to Budišin’s construction. Actually, from the viewpoint of the PU matrices, the construction in [9] is identical to our construction in [52], but they were not aware of our work [52] until 2018. A hardware implementation, an enumeration of the sequences, and a comparison with known constructions of CCCs in [29], [46] were also given in [9]. Furthermore, we have showed in [27] that the new sequences in CSSs of size 4 can be obtained by the PU-matrix-based construction [52]. However, the relationship between the sequences constructed by PU-matrix-based method and GBF-based method is unsolved until now.

The concept of GSP was generalized to Golay array pair (GAP) in [25], which has found applications in coded imaging [12]. A powerful three-stage process was presented in [25] by showing that all known GSPs of length \( 2^m \) can be derived from the seed GAPs.

In this paper, inspired by the excellent idea introduced in [15], [18], [32], we generalize the concepts of CSS and CCC to a complementary array set (CAS) and a complete complementary array (CCA), and show that a large number of CSSs and CCCs of size \( N \) can be constructed from a single CCA of size \( N \). We also prove that a CCA of size \( N \) can be constructed by a multivariate polynomial matrix of order \( N \) satisfying some properties, which is referred to as a desired PU matrix in this paper. A principal objective of this paper is to construct desired PU matrices together with extracting the explicit forms of the functions (arrays) from the desired PU matrices. Consequently, CSSs and CCCs can be constructed from these functions. The proposed constructions from desired PU matrices in this paper not only generate new CSSs and CCCs, but also reveal that the known constructions of CSSs and CCCs of length \( 2^m \) [10], [33], [38], [42] are special cases of those constructions.

Since this paper consists of a large volume of the contents, in order to easily read the paper, in the following we provide a summary of our main contributions of this paper together with their dependency relationships among our new constructions.

1) We introduce a general framework for constructing desired PU matrices (Theorem 1 in Section III) and a general treatment of sequences, arrays, and their respective generating functions.

2) By extending the univariate PU matrices in [52] to the array version, we obtain the first construction of the desired PU matrices in this paper, which is called seed PU matrices (Theorem 2 in Section IV). More precisely, such a seed PU matrix is constructed by iteratively multiplying \( m \) times the product of BH matrices and a delay matrix to the BH matrices.

a) One important contribution of this paper is to provide a systematic approach to extract the functions (arrays) from the seed PU matrices. These functions depend on a basis of functions from \( \mathbb{Z}_N \) to \( \mathbb{Z}_q \) and representatives in the equivalence class of BH matrices.

b) From this construction, all the functions fill up a larger number of cosets of a linear code. Furthermore, since the newly constructed functions from the seed PU matrices in this paper also determine all the sequences from PU-matrix-based constructed in [9], [29], [46], [52], our enumeration based on a rigorous proof corrects some results in [9].

3) Using the construction from the seed PU matrices (Theorem 5 in Subsection IV-E), we realize four different classes of CCAs and the sequences with the explicit function forms in both CSSs and CCCs in Section V, which are summarized as follows.

a) For q-ary pair \( (N = q = 2, q = 3 \) is even), our Construction 1 exactly coincides with the standard GSPs [10] by Davis and Jedwab.

b) For the case size 3 \( (N = 2, q = 3) \), there are \( m! \cdot 2^{m^2-2} \cdot 3^{2m+1} \) new constructed ternary sequences in CSSs of 3.

c) For respective binary and quaternary cases of size 4 \( (N = 4, q = 2 \) and \( q = 4 \) ), these binary and quaternary sequences can be represented by explicit GBFs in a general form respectively. Both binary and quaternary sequences fill up a large
number of cosets of a linear code $\delta_L(q, 4)$ for $q = 2$ and $q = 4$ respectively, which contains the first-order GRM code as a sub-code. For $q = 2$, the sequences can be explained by the results in [54]. However, for $q = 4$, most of them are never reported before. Note that sequences in CSSs of size 4 have been deeply studied for PMEPR control for almost 20 years.

4) However, the construction using the seed PU matrices cannot explain all the known constructions. We then turn our focus to the arrays of size $2 \times 2 \times \cdots \times 2$. We generalize the seed PU matrices of order $N = 2^n$, where the delay matrix in a seed PU matrix in Theorem 2 is replaced by a generalized delay matrix, which is the Kronecker product of $n$ delay matrices of order 2 (Theorem 6 in Section VI). And the explicit GBF forms are derived in Theorem 7 (in Section VI). This result extends the univariate PU matrices in [26] to the array version and determines the GBF forms of the sequences derived from generalized seed PU matrices.

5) Following (generalized) seed PU matrices, we introduce two basic recursive PU-matrix-based constructions from seed PU matrices of order 2 (or GAPs). Roughly speaking, the first one is the product of two PU matrices of order $2^{n+1}$ where the multiplier is a block diagonal matrix of order $2^{n+1}$ by two BH matrices of order $2^n$ as diagonal matrices, and the multiplicand is constructed using $n$ seed PU matrices of order 2 to form a block diagonal matrix of order $2^{n+1}$ (Theorem 8 in Subsection VII-A). The second one is the product of three matrices: one is from the PU matrix in Theorem 8, the second is a block diagonal matrix with two generalized delay matrices as the diagonal matrices, and the third is a block diagonal matrix with two BH matrices as the diagonal matrices (Theorem 9 in Subsection VII-A). Then we show that the known GBF-based constructions of CSSs by Paterson [33] and by Schmidt [42] and CCCs by Rathinakumar and Chaturvedi [38] can be constructed by the PU-matrix-based constructions in Subsection VII-B, where all BH matrices involved are the WHT (Walsh-Hadamard transform) matrices. We further generalize the above recursive constructions on CSSs and CCCs (Theorems 10 and 11 in Subsection VII-C). Those results can be used in bounding the PMEPR.

Basically, we have explicitly showed that the known constructions of CSSs and CCCs in [10], [33], [38], [42] can be constructed by our method only involving in seed PU matrices of order 2, or equivalently, these results on CSSs and CCCs can be constructed from the WHT matrices. On the other hand, there are two different equivalent class for quaternary BH matrices of order 4. One is equivalent to the WHT matrix, and the other is equivalent to the DFT (Discrete Fourier transform) matrix. It has been verified in our Construction 4 (in Subsection V-D) that any sequences related to the DFT matrix of order 4 were not reported before. Thus, the results for the seed PU matrices of order 4, combined with the recursive constructions in this paper, significantly increase the number of the quaternary sequences in CSSs of size 4. Moreover, there are 15 equivalent classes of quaternary BH matrices of order 8, and 319 equivalent classes of BH matrices of order 12. Thus, the observation by taking all the BH matrices into consideration sheds light on the PMEPR control problem by codes with higher rate. It is expected that the results presented in this paper suggest that we should go back to the first paper for CSSs [49] where the CSSs are constructed by the Hadamard matrices of order $N$ for finding more new CSSs and CCCs.

The rest of our paper is organized as follows. In the next section, we introduce most of our notations, give a brief viewpoint of $m$-dimensional arrays, and define the concepts of CCA, CCC, CAS and CSS. The evaluation from an array to a sequence which gives a way from a CCA to a large number of CCCs and CSSs is also given. In Section III, we introduce desired PU matrices, BH matrices and their equivalence relationship. In Section IV, we propose a construction of seed PU matrices, and develop a systematic approach to extract the explicit form of functions and sequences from seed PU matrices. Binary sequences in GSPs, ternary sequences in CSSs of size 3, binary and quaternary sequences in CSSs of size 4 are provided in Section V. The results for seed PU matrices of order $2^n$ are generalized in Section VI. We develop a general method to construct the desired PU matrices, and present a framework to recursively construct CCCs and CSSs in Sections VII. We conclude the paper with some open problems in Section VIII.

II. PRELIMINARIES

In this section, we introduce the notations of sequence and array, and define the concepts of CCA, CCC, CAS and CSS. The evaluation from an array to a sequence gives our perspective on how to construct a large number of CSSs and CCCs from a single CCA. The following notations will be used throughout the paper.

- For integer $p$, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ is the residue class ring modulo $p$. $\mathbb{Z}_p^*$ denotes $\mathbb{Z}_p\setminus\{0\}$.
- For function $f(y) = f(y_0, y_1, \ldots, y_{m-1})$ from $\mathbb{Z}_p^m$ to $\mathbb{Z}_q$, the action of permutation $\pi$ on the function $f(y)$, denoted as $\pi \cdot f$, is defined by $\pi \cdot f(y) = f(\pi(y_0), \pi(y_1), \ldots, \pi(y_{m-1}))$.
- If $y_k$ is a Boolean variable, i.e., $y_k \in \mathbb{Z}_2$, it is replaced by $x_k$, and $f(y)$ is replaced by $f(x)$ in this paper.
- $\omega = e^{2\pi i/q}$ is a $q$th primitive root of unity.
- $I_N$ and $J_N$ denote the identity matrix and all 1 matrix of order $N$, respectively.

A. Sequences, Arrays and Generating Functions

A $q$-ary sequence $f$ of length $L$:

$$f = (f(0), f(1), \ldots, f(L-1)),$$

can be represented by a function

$$f(t) : \mathbb{Z}_L \to \mathbb{Z}_q,$$
which is referred to as the corresponding function of sequence \( f \). Moreover, the sequence \( f \) can be associated with a polynomial defined by

\[
F(Z) = \sum_{t=0}^{L-1} \omega^{f(t)} Z^t.
\]  

The polynomial \( F(Z) \) is called the generating function of sequence \( f \).

Note that both the corresponding function \( f(t) \) and the generating function \( F(Z) \) are uniquely determined by the sequence \( f \), and vice versa. So we can use either the corresponding function \( f(t) \) or the generating function \( F(Z) \) to represent a sequence \( f \).

The above concepts about sequences were extended to arrays in [15]. An \( m \)-dimensional \( q \)-ary array of size \( p \times p \times \cdots \times p \) can be represented by a corresponding function, which is a multivariate polynomial function mapping from \( \mathbb{Z}_p^m \) to \( \mathbb{Z}_q \):

\[
f(y) = f(y_0, y_1, \cdots, y_{m-1}) : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q
\]

for \( y = (y_0, y_1, \cdots, y_{m-1}) \) and \( y_k \in \mathbb{Z}_p \). So in this paper, an \( m \)-dimensional \( q \)-ary array of size \( p \times p \times \cdots \times p \) corresponds to a multivariate polynomial function \( f(y_0, y_1, \cdots, y_{m-1}) \) mapping from \( \mathbb{Z}_p^m \) to \( \mathbb{Z}_q \).

In particular, if \( p = 2 \), an \( m \)-dimensional \( q \)-ary array of size \( 2 \times 2 \times \cdots \times 2 \) can be realized by a generalized Boolean function (GBF):

\[
f(x) = f(x_0, x_1, \cdots, x_{m-1}) : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_q.
\]

The (multivariate) generating function of array \( f(y) = f(y_0, y_1, \cdots, y_{m-1}) \) is defined by

\[
F(z) = \sum_{y_0=0}^{p-1} \sum_{y_1=0}^{p-1} \cdots \sum_{y_{m-1}=0}^{p-1} \omega^{f(y_0, y_1, \cdots, y_{m-1})} z_0^{y_0} z_1^{y_1} \cdots z_{m-1}^{y_{m-1}}.
\]  

The term \( z_0^{y_0} z_1^{y_1} \cdots z_{m-1}^{y_{m-1}} \) is denoted by \( z^y \) for short in the whole paper, where \( z = (z_0, z_1, \cdots, z_{m-1}) \).

From the definition above, a sequence \( f(t) : \mathbb{Z}_L \rightarrow \mathbb{Z}_q \) can be regarded as an array of dimension 1.

### B. CSS and CCC

In this subsection, we introduce the definitions of CSS and CCC from the viewpoints of aperiodic correlation and the generating functions of the sequences, respectively.

**Definition 1:** For two \( q \)-ary sequences \( f_1 \) and \( f_2 \) of length \( L \), the aperiodic cross-correlation of \( f_1 \) and \( f_2 \) at shift \( \tau \) \((-L < \tau < L)\) is defined by

\[
C_{f_1,f_2}(\tau) = \begin{cases} 
L-1-\tau & \text{if } \tau < 0, \\
\sum_{t=0}^{L-1-\tau} \omega^{f_1(t+\tau)-f_2(t)}, & 0 \leq \tau < L, \\
\sum_{t=0}^{L-1+\tau} \omega^{f_1(t)-f_2(t-\tau)}, & -L < \tau < 0.
\end{cases}
\]

If \( f_1 = f_2 = f \), the aperiodic autocorrelation of sequence \( f \) at shift \( \tau \) is denoted by

\[
C_f(\tau) = C_{f,f}(\tau).
\]

**Definition 2:** A set of sequences \( S = \{ f_0, f_1, \cdots, f_{N-1} \} \) is called a complementary sequence set (CSS) of size \( N \) if

\[
\sum_{\tau=0}^{N-1} C_{f_j}(\tau) = 0 \quad \text{for } \tau \neq 0.
\]

If the set size \( N = 2 \), such a set is called a Golay sequence pair (GSP). Each sequence in GSP is called a Golay sequence.

Two CSSs \( S_1 = \{ f_1, f_2, \cdots, f_{N-1} \} \) and \( S_2 = \{ f_1, f_2, \cdots, f_{N-1} \} \) are said to be mutually orthogonal if

\[
\sum_{\tau=0}^{N-1} C_{f_{1,j},f_{2,j}}(\tau) = 0, \quad \forall \tau.
\]

The number of CSSs which are pairwise mutually orthogonal is at most equal to \( N \), the number of sequences in a CSS.

**Definition 3:** Let \( S_i = \{ f_{i,0}, f_{i,1}, \cdots, f_{i,N-1} \} \) be CSSs of size \( N \) for \( 0 \leq i < N \), which are pairwise mutually orthogonal. Such a collection of \( S_i \) is called complete mutually orthogonal complementary sets (CMOCS) or complete complementary codes (CCC).

The concept of CCC is better to view through a matrix. Let \( S \) be a matrix where the \( i \)-th row is given by \( S_i \), i.e.,

\[
S = \begin{bmatrix}
f_{0,0} & f_{0,1} & \cdots & f_{0,N-1} \\
f_{1,0} & f_{1,1} & \cdots & f_{1,N-1} \\
\vdots & \vdots & \ddots & \vdots \\
f_{N-1,0} & f_{N-1,1} & \cdots & f_{N-1,N-1}
\end{bmatrix}.
\]

Then \( \{ f_{i,j} \}_{0 \leq i,j < N} \) is a CCC if and only if every row of the matrix \( S \) is a CSS of size \( N \), and any two rows are mutually orthogonal.

**Example 1:** For \( q = 4, N = 2 \) and \( L = 4 \), a matrix of sequences given by

\[
S = \begin{bmatrix}
(0, 1, 0, 3) & (0, 1, 2, 1) \\
(0, 3, 0, 1) & (0, 3, 2, 3)
\end{bmatrix}
\]

form a CCC of size \( 2 \).

A useful tool for studying CSS and CCC is the generating function \( F(Z) \) of the sequence \( f \). We denote the complex conjugate of \( F(Z) \) by \( \overline{F}(Z) \), i.e.,

\[
\overline{F}(Z) = \sum_{t=0}^{L-1} \omega^{-f(t)} Z^t.
\]

Suppose that \( F_1(Z) \) and \( F_2(Z) \) are the generating functions of sequences \( f_1 \) and \( f_2 \), respectively. It is easy to verify

\[
F_1(Z)\overline{F}_2(Z^{-1}) = \sum_{\tau=1}^{N-1} C_{f_1,f_2}(\tau)Z^\tau.
\]

Then \( S = \{ f_0, f_1, \cdots, f_{N-1} \} \) forms a CSS if and only if their generating functions \( \{ F_0(Z), F_1(Z), \cdots, F_{N-1}(Z) \} \) satisfy

\[
\sum_{j=0}^{N-1} F_j(Z)\overline{F}_j(Z^{-1}) = NL.
\]
Moreover, two CSSs $S_1 = \{ f_{1,0}, f_{1,1}, \cdots, f_{1,N-1} \}$ and $S_2 = \{ f_{2,0}, f_{2,1}, \cdots, f_{2,N-1} \}$ are mutually orthogonal if and only if their respective generating functions $\{ F_{i,0}(Z), F_{i,1}(Z), \cdots, F_{i,N-1}(Z) \}$ $(i = 1, 2)$ satisfy
\[ \sum_{j=0}^{N-1} F_{i,j}(Z) \overline{F_{2,j}(Z^{-1})} = 0. \tag{8} \]

Thus the conditions given in the equations (3) and (4), defined by aperiodic correlation of the sequences, are equivalent to the conditions in (7) and (8) defined by their generating functions.

C. CAS and CCA

In this subsection, we generalize the concepts of CSS and CCC to CAS and CCA, respectively.

Definition 4: Let $f_1(y)$ and $f_2(y)$ be two arrays from $\mathbb{Z}_p^n$ to $\mathbb{Z}_q$. The aperiodic cross-correlation of arrays $f_1$ and $f_2$ at shift $\tau = (\tau_0, \tau_1, \cdots, \tau_{m-1})$ $(1 - p \leq \tau_k \leq p - 1)$ is defined by
\[ C_{f_1, f_2}(\tau) = \sum_{y \in \mathbb{Z}_p^n} \omega^{f_1(y+\tau)-f_2(y)}, \]
where $\omega = e^{2\pi i / q}$ is the element-wise addition of vectors over $\mathbb{Z}_q$ and $\omega^{f_1(y+\tau)-f_2(y)} = 0$ if $f_1(y+\tau)$ or $f_2(y)$ is not defined.
If $f_1 = f_2 = f$, then it is called the aperiodic autocorrelation of array $f$ at shift $\tau$, denoted by
\[ C_f(\tau) = C_{f,f}(\tau). \]

Suppose that $F_1(z)$ and $F_2(z)$ are the generating functions of arrays $f_1(y)$ and $f_2(y)$, respectively. Here we denote $z^{-1} = (z_0^{-1}, z_1^{-1}, \cdots, z_{m-1}^{-1})$ for short. Similar to the case of sequence, we have
\[ F_1(z) \cdot F_2(z^{-1}) = \sum_{\tau} C_{f_1, f_2}(\tau) z_0^{\tau_0} z_1^{\tau_1} \cdots z_{m-1}^{\tau_{m-1}}. \tag{9} \]

Definition 5: A set of arrays $\{ f_0, f_1, \cdots, f_{N-1} \}$ from $\mathbb{Z}_p^n$ to $\mathbb{Z}_q$ is called a complementary array set (CAS) of size $N$ if their generating functions $\{ F_0(z), F_1(z), \cdots, F_{N-1}(z) \}$ satisfy
\[ \sum_{j=0}^{N-1} F_j(z) \cdot F_j(z^{-1}) = N \cdot p^m. \tag{10} \]

If the set size $N = 2$, such a set is called a Golay array pair (GAP). Each array (i.e., the function) in GAP is called a Golay array.

Two CASs $S_1 = \{ f_{1,0}, f_{1,1}, \cdots, f_{1,N-1} \}$ and $S_2 = \{ f_{2,0}, f_{2,1}, \cdots, f_{2,N-1} \}$ are said to be mutually orthogonal if their generating functions $\{ F_{i,0}(z), F_{i,1}(z), \cdots, F_{i,N-1}(z) \}$ $(i = 1, 2)$ satisfy
\[ \sum_{j=0}^{N-1} F_{i,j}(z) \overline{F_{2,j}(z^{-1})} = 0. \tag{11} \]

Definition 6: Let $S_i = \{ f_{i,0}, f_{i,1}, \cdots, f_{i,N-1} \}$ $(0 \leq i < N)$ be CASs of size $N$, which are pairwise mutually orthogonal. We call such a collection of $S_i$ $(0 \leq i < N)$ a complete mutually orthogonal array set or a complete complementary arrays (CCA).

\[ f(y) \leftarrow F(z) = \sum_{y} \omega^{f(y)} z^y \rightarrow F(z) \]
\[ t = \sum_{k=0}^{m-1} y_k \cdot p^k \]
\[ z_k = Z^{p^k} \]

Fig. 1. Arrays, sequences, and their generating functions.

Remark 1: It is obvious that the equation (10) is equivalent to
\[ \sum_{j=0}^{N-1} C_{f_j}(\tau) = 0 \]
for $\forall \tau \neq 0$, and the equation (11) is equivalent to
\[ \sum_{j=0}^{N-1} C_{f_{i,j}, f_{2,j}}(\tau) = 0 \]
for $\forall \tau$.

D. Relationship Between Arrays and Sequences

We specify a sequence $f(t) : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q$ corresponding to an array $f(y) : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_q$ by listing the values of $f(y)$ in lexicographic order, i.e.,
\[ f(t) = f(y) \text{ for } t = \sum_{k=0}^{m-1} y_k \cdot p^k. \]
We say that the sequence $f(t)$ is evaluated by the function (or array) $f(y)$ in this paper.

For an array $f(y) : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q$ and its evaluated sequence $f(t) : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q$, their respective generating functions $F(z)$ and $F(Z)$ can be connected by restricting $z_k = Z^{p^k}$. The derivation is given as follows:

\[ F(z) = F(Z^{p^0}, Z^{p^1}, \cdots, Z^{p^{m-1}}) = \sum_{y_0, y_1, \cdots, y_{m-1}} \omega^{f(y)} \cdot Z^{y_0 p^0} Z^{y_1 p^1} \cdots Z^{y_{m-1} p^{m-1}} = \sum_{t=0}^{L-1} \omega^{f(t)} \cdot Z^t \]
\[ = F(Z). \]

The above discussions are summarized in Figure 1.

Example 2: For $q = 4$, $p = m = 2$, let $\omega = e^{\pi i \sqrt{3}}$ be a 4th primitive root of unity and GBF \( f(x) = f(x_0, x_1) = 2 x_0 x_1 + x_0 \). The generating function of array $f(x)$ is given by
\[ F(z) = F(z_0, z_1) = \omega^0 + \omega^1 z_0 + \omega^0 z_1 + \omega^3 z_0 z_1. \]
The sequence evaluated by the GBF $f(x)$ is $f = (0, 1, 0, 3)$ with generating function
\[ F(Z) = \omega^0 + \omega^1 Z + \omega^0 Z^2 + \omega^3 Z^3. \]
It is clear that $F(z) = F(Z)$ by setting $z_0 = Z$ and $z_1 = Z^2$. 
Thus, if \( \{f_0, f_1, \cdots, f_{N-1}\} \) constitutes a CAS, then its evaluated sequences constitute a CSS. Moreover, recall the action of permutation \( \pi \) on the array:

\[
\pi \cdot f = f(\pi(0))y_{\pi(1)}\cdots y_{\pi(m-1)}.
\]

Since the equations (10) and (11) still hold if we apply action of a permutation on the arrays, it is easy to know that the set \( \{f_0, f_1, \cdots, f_{N-1}\} \) is a CAS if and only if \( \{\pi \cdot f_0, \pi \cdot f_1, \cdots, \pi \cdot f_{N-1}\} \) is also a CAS.

Property 1: For any permutation \( \pi \),

(1) if a set of arrays \( \{f_0, f_1, \cdots, f_{N-1}\} \) is a CAS, then the sequences evaluated by functions \( \{\pi \cdot f_0, \pi \cdot f_1, \cdots, \pi \cdot f_{N-1}\} \) form a CSS; and

(2) if \( S_i = \{f_{i,0}, f_{i,1}, \cdots, f_{i,N-1}\} \) \( 0 \leq i < N \) is a CCA, the sequences evaluated by functions \( S'_i = \{\pi \cdot f_{i,0}, \pi \cdot f_{i,1}, \cdots, \pi \cdot f_{i,N-1}\} \) \( 0 \leq i < N \) form a CCA.

From Property 1, we can construct a large number of CSSs from a CAS (or a large number of CCCs from a CCA). This is one of the main reasons that we study the CSSs and CCCs through CASs and CCAs.

E. Special Case for \( p = 2 \)

We set \( p = 2 \) in this subsection. For GBFs \( f_1, f_2, \) and any affine GBF

\[
f' = \sum_{k=0}^{m-1} c_k x_k + c' (c_k, c' \in \mathbb{Z}_q)
\]

we have

\[
C_{f_1+f', f_2+f'}(\tau) = \omega^{f(\tau)}c' C_{f_1, f_2}(\tau).
\]

(12)

Then the following assertions are immediately obtained from the definitions.

Property 2: For any permutation \( \pi \) and affine function \( f' \),

(1) if a set of GBFs \( \{f_0, f_1, \cdots, f_{N-1}\} \) is a CAS, the sequences evaluated by \( \{\pi \cdot f_0 + f', \pi \cdot f_1 + f', \cdots, \pi \cdot f_{N-1} + f'\} \) form a CSS; and

(2) if \( S_i = \{f_{i,0}, f_{i,1}, \cdots, f_{i,N-1}\} \) \( 0 \leq i < N \) is a CCA, the sequences evaluated by functions \( S'_i = \{\pi \cdot f_{i,0} + f', \pi \cdot f_{i,1} + f', \cdots, \pi \cdot f_{i,N-1} + f'\} \) \( 0 \leq i < N \) form a CCA.

Note that the above property was proved in [15, Lemma 8] for the pair case. Moreover, the three-stage process in [15] is simplified by the process from the array \( f \) to the sequences evaluated by \( (\pi \cdot f + f') \) in this paper.

From Property 2, we can construct a large number of CSSs (or CCCs) from a CAS (or CCA). On the other hand, the set \( \{\pi \cdot f + f'\} \), where \( \pi \) can be any permutation and \( f' \) can be any affine GBF, must be comprised of some cosets of the first-order GRM code. This is another strong supporting evidence that we investigate the constructions for CSSs through the constructions of CASs.

For a given GBF \( f \), let \( N_0 \) be the number of pairs \( (\pi, f') \) such that \( \pi \cdot f + f' = f \), and \( N_1 \) be the number of functions in the set \( \{\pi \cdot f + f'\} \). From the orbit-stabilizer theorem [43], the set \( \{\pi \cdot f + f'\} \) contains \( N_1 = \frac{n!}{N_0} \) GBFs.

Example 3: Let \( q \) be an even integer. It is known that Rudin-Shapiro function \( f(x) = \frac{q}{2} \sum_{k=0}^{m-2} x_k x_{k+1} + 1 \) and \( f(x) + \frac{q}{2} x_0 \) form a GAP. From Property 2, the sequences evaluated by

\[
\pi \cdot f + f' = \frac{q}{2} \sum_{k=1}^{m-1} x_{\pi(k)} x_0 + \sum_{k=0}^{m-1} c_k x_k + c',
\]

form a GSP for \( c_k, c' \in \mathbb{Z}_q \), which agrees with the standard Golay pair in [10]. Moreover, the number of the standard Golay sequences can be calculated by \( N_1 = \frac{1}{2} m! q^{m+1} \) for \( N_0 = 2 \).
A. Multivariate Para-Unitary Matrices and CCA

A multivariate para-unitary matrix is straightforwardly generalized from a univariate para-unitary matrix, which plays a central role in signal processing, in particular in the areas of filter banks and wavelets.

Definition 7: Let $M(z)$ be a square multivariate polynomial matrix of order $N$. If

$$M(z) \cdot M^\dagger(z^{-1}) = c \cdot I_N,$$

where $(\cdot)^\dagger$ denotes the Hermitian transpose and $c$ is a real constant. We say that $M(z)$ is a multivariate para-unitary (PU) matrix.

Note that the entries of a PU matrix may not be able to map to the polyphase arrays. Recall the definitions of function matrices and generating matrices in (13) and (14), respectively. In this paper, a PU matrix $M(z)$ is called a desired PU matrix if it is the generating matrix of a function matrix $\tilde{M}(y)$, i.e., each entry of $M(z)$ can be expressed by

$$M_{i,j}(z) = \sum_{y} \omega^{f_{i,j}(y)} z^y,$$

where $\omega$ is the $q$th primitive root of unity and $f_{i,j}(y)$ is a function from $\mathbb{Z}_p^m$ to $\mathbb{Z}_q$.

A large number of CSSs and CCCs can be constructed from a desired PU matrix according to the following theorem.

Theorem 1: If $M(z)$ is a desired PU matrix with corresponding function matrix $\tilde{M}(y)$, we have

1. The arrays $\{f_{i,j}(y)\}$ in function matrix $\tilde{M}(y)$ form a CCA.
2. The sequences evaluated by the functions in matrix $\pi \cdot \tilde{M}(y)$ form a CCC for any $\pi$.
3. The arrays $\{f_{i,j}(y)\}$ in each row (or column) of $\tilde{M}(y)$ form a CAS.
4. The sequences evaluated by the functions in each row (or column) of the matrix $\pi \cdot \tilde{M}(y)$ form a $q$-ary CSS of size $N$ and length $p^m$ for any $\pi$.
5. If $p = 2$, for any affine GBF $f'$ and permutation $\pi$, the sequences evaluated by the functions in $(\pi \cdot \tilde{M}(x) + f'(x) \cdot J_N)$ form a CCC, and the sequences evaluated by the functions in each row (or column) of the matrix $(\pi \cdot \tilde{M}(x) + f'(x) \cdot J_N)$ form a $q$-ary CSS of size $N$ and length $2^m$.

One principal objective of this paper is to find some desired PU matrices. However, each entry of a desired PU matrix $M(z)$ is a multivariate polynomial over the complex field, but not a function from $\mathbb{Z}_p^m$ to $\mathbb{Z}_q$. So another principal objective of this paper is to exact the function matrix $\tilde{M}(y)$ from its generating matrix $M(z)$.

B. Butson-Type Hadamard Matrices

A complex Hadamard matrix of order $N$ is a complex matrix $H$ satisfying $|H_{i,j}| = 1 \ (0 \leq i,j < N)$ and $H \cdot H^\dagger = N \cdot I_N$. A complex Hadamard matrix $H$ is called Butson-type [5] if all the entries of $H$ are $q$th roots of unity, i.e., $H = \{H_{i,j}\}_{N \times N}$ where $H_{i,j} = \omega^{\bar{H}_{i,j}}$ for $\bar{H}_{i,j} \in \mathbb{Z}_q$. For fixed $N$ and $q$, we denote the set of all Butson-type Hadamard (BH) matrices by $H(q,N)$.

It is obvious that the BH matrix is the simplest desired PU matrix $(p = m = 1)$, i.e., the entry of the desired PU matrix is associated with a sequence of length 1.

Two BH matrices, $H_1, H_2 \in H(q,N)$ are called equivalent, denoted by $H_1 \simeq H_2$, if there exist diagonal unitary matrices $Q_1, Q_2$, where each diagonal entry is a $q$th root of unity, and permutation matrices $P_1, P_2$ such that:

$$H_1 = Q_1 \cdot P_1 \cdot H_2 \cdot P_2 \cdot Q_2.$$

(17)

Example 4: For $q$ odd, $H(q,2) = \emptyset$. For $q$ even, all Hadamard matrices in $H(q,2)$ are equivalent to the WHT matrix of order 2:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

We introduce the Kronecker product of matrices.

Definition 8: If $A = \{a_{i,j}\}$ is a square matrix of order $n_1$ and $B$ is a square matrix of order $n_2$, then the Kronecker product $A \otimes B$ is a block matrix of order $n_1 \cdot n_2$, given by

$$A \otimes B = \begin{bmatrix} a_{0,0} \cdot B & a_{0,1} \cdot B & \ldots & a_{0,n_1-1} \cdot B \\ a_{1,0} \cdot B & a_{1,1} \cdot B & \ldots & a_{1,n_1-1} \cdot B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_1-1,0} \cdot B & a_{n_1-1,1} \cdot B & \ldots & a_{n_1-1,n_1-1} \cdot B \end{bmatrix}.$$

Example 5: All binary Hadamard matrices in $H(2,4)$ are equivalent to the WHT matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix},$$

which is the Kronecker product of WHT matrix of order 2.

Example 6: All quaternary BH matrices in $H(4,4)$ are equivalent to one of the following two BH matrices:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \sqrt{-1} & -1 & \sqrt{-1} \\ 1 & -1 & 1 & -1 \\ 1 & -\sqrt{-1} & -1 & \sqrt{-1} \end{bmatrix},$$

i.e., the WHT matrix and the DFT matrix of order 4.

C. Phase Matrices of Hadamard Matrices

For a BH matrix $H = \{H_{i,j}\} \in H(q,N)$, we can define its phase matrix $\bar{H} = \{\bar{H}_{i,j}\}_{N \times N}$ by $H_{i,j} = \omega^{\bar{H}_{i,j}}$. Actually, BH matrix $H$ can be treated as a desired PU matrix and the phase matrix $\bar{H}$ is its corresponding function matrix. For given $N$ and $q$, we denote $H(q,N)$ the set consisting of all phase matrices of BH matrices.

Definition 9: Let $\bar{H}_1$ and $\bar{H}_2$ be two phase matrices induced by BH matrices $H_1$ and $H_2$, respectively. The equivalence of the phase matrices is defined by the equivalence of the Hadamard matrices, i.e., $\bar{H}_1 \simeq \bar{H}_2$ if and only if $H_1 \simeq H_2$. 
Example 7: For $q$ odd, $\tilde{H}(q, 2) = \emptyset$. For $q$ even, all phase matrices in $\tilde{H}(q, 2)$ are equivalent to

$$
\begin{bmatrix}
0 & 0 \\
q/2 & 0
\end{bmatrix}.
$$

Example 8: All binary phase matrices in $\tilde{H}(2, 4)$ are equivalent to the $4 \times 4$ phase matrix:

$$
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0
\end{bmatrix}.
$$

Example 9: All quaternary phase matrices in $\tilde{H}(4, 4)$ are equivalent to one of the following two $4 \times 4$ phase matrices:

$$
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 2 & 0 & 2 \\
0 & 0 & 2 & 2 \\
0 & 2 & 2 & 0
\end{bmatrix} \quad \text{and} \quad
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 \\
0 & 2 & 0 & 2 \\
0 & 3 & 2 & 1
\end{bmatrix}.
$$

The representatives of the equivalent classes in $\tilde{H}(q, N)$ play a crucial role in the process of extracting functions from the desired PU matrix in this paper. We denoted $\tilde{S}_P(q, N)$ the set consisting of all the representatives of the equivalent classes of the phase matrices.

IV. SEED PU MATRICES AND CORRESPONDING FUNCTION MATRICES

In this section and the next section, we always assume $N = p$. We will first introduce a construction of the desired PU matrices, and then develop an approach to study the explicit function forms of arrays in corresponding function matrices.

A. Construction of Seed PU Matrices

Let $D(z)$, called the delay matrix, be a $p$ by $p$ diagonal matrix with the form $D(z) = \text{diag}(z^0, z^1, z^2, \ldots, z^{p-1})$, i.e.,

$$
D(z) = \begin{bmatrix}
0 & 0 & 0 & \cdots & 0 \\
0 & z^1 & 0 & \cdots & 0 \\
0 & 0 & z^2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & z^{p-1}
\end{bmatrix}.
$$

Let $H_k$ be an arbitrary BH matrix chosen from $H(q, N)$ for $0 \leq k \leq m$. Define a multivariate polynomial matrix $M(z)$ as follow.

$$
M(z) = H_0 \cdot D(z_0) \cdot H_1 \cdot D(z_1) \cdot \cdots \cdot \left( \prod_{k=0}^{m-1} H_k \cdot D(z_k) \right) \cdot H_m.
$$

Theorem 2: $M(z)$ defined above is a desired PU matrix, i.e.,

1. $M(z) \cdot M^T(z^{-1}) = N^{m+1} \cdot I_N$;

2. Each entry of $M(z)$ can be expressed by the generating function of an array $f(y) : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q$.

$M(z)$ defined in (19) is called the seed PU matrix in this paper.

B. The Proof of Theorem 2

The first assertion in Theorem 2 on the para-unitary condition follows from

$$
H^k \cdot H^{k\dagger} = N \cdot I_N
$$

and

$$
D(z_k) \cdot D^T(z_k^{-1}) = I_N.
$$

According to formula (16), $M(z)$ can be expanded in the form

$$
M(z) = \sum_{y \in \mathbb{Z}_p^m} M(y) z^y.
$$

Note that the second assertion in Theorem 2 is valid if and only if all the entries of $M(y)$ are $q$th roots of unity for $y \in \mathbb{Z}_p^m$.

Let $E_{yk}$ be a matrix with single-entry 1 at $(i, i)$ and zero elsewhere. The coefficient matrices $M(y)$ can be determined by the following lemma.

**Lemma 1:** The coefficient matrix $M(y)$ can be determined by BH matrices as follow.

$$
M(y) = \prod_{k=0}^{m-1} \left( H_k \cdot E_{yk} \right) \cdot H_m.
$$

**Proof:** We write the delay matrix $D(z_k)$ in the form

$$
D(z_k) = \sum_{y_k=0}^{p-1} E_{yk} z_k^{y_k}.
$$

Then multivariate polynomial matrix $M(z)$ can be re-expressed as follows.

$$
M(z) = \left( \prod_{k=0}^{m-1} \left( H_k \cdot D(z_k) \right) \right) \cdot H_m
$$

$$
= \left( \prod_{k=0}^{m-1} \left( H_k \cdot \sum_{y_k=0}^{p-1} E_{yk} z_k^{y_k} \right) \right) \cdot H_m
$$

$$
= \left( \sum_{y \in \mathbb{Z}_p^m} \prod_{k=0}^{m-1} \left( H_k \cdot E_{yk} \right) \cdot H_m \right) z^y.
$$

We complete the proof according to the expansion of $M(z)$ in (20).

**Lemma 2:** Let $M_{ij}(y)$ be the entry of the coefficient matrix $M(y)$ at $(i, j)$. Then $M_{ij}(y)$ must be a product of some entries of BH matrices $H_k$. More precisely, we have

$$
M_{i,j}(y_0, y_1, \ldots, y_{m-1}) = H^{(i)}_{i,y_0} \left( \prod_{k=1}^{m-1} H^{(k)}_{y_k-1,y_k} \right) \cdot H^{(m)}_{y_{m-1},j}.
$$
Proof: It follows from Lemma 1 and $E_{0k}$ being a matrix with single-entry 1 at $(y_k, y_k)$ and zero elsewhere.

According to Lemma 2, we know that $M_{i,j}(y)$ must be a $q^{th}$ root of unity, denoted by $M_{i,j}(y) = \omega^{j(i,y)}$. Then each entry of $M(z)$ can be written in the form

$$M_{i,j}(z) = \sum_{y \in \mathbb{Z}_q^n} M_{i,j}(y)z^y = \sum_{y \in \mathbb{Z}_q^n} \omega^{j(i,y)}z^y,$$

which completes the proof of Theorem 2.

Remark 2: If we restrict $z_k = Z_q^{p(k)}$ in the multivariate seed PU matrices in this subsection, we obtain the univariate PU matrices proposed in [9], [52].

C. Extracting Functions From the Seed PU Matrices

In this subsection, we give a general form of functions $f_{i,j}(y)$ in (22) from the seed PU matrices. The proofs and the approach on how to extract these functions will be shown in the next subsection.

We first introduce Kronecker-delta functions from $\mathbb{Z}_N$ to $\mathbb{Z}_q$.

Definition 10: Let $\delta_i$ be a function: $\mathbb{Z}_N \rightarrow \mathbb{Z}_q$ such that $\delta_i(j) = \delta_{ij}$ where $\delta_{ij}$ is the Kronecker-delta function, i.e.,

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Kronecker-delta functions form a basis of the functions from $\mathbb{Z}_N$ to $\mathbb{Z}_q$. Any function $g: \mathbb{Z}_N \rightarrow \mathbb{Z}_q$ can be represented by

$$g = \sum_{i=0}^{N-1} g(i)\delta_i.$$  

Example 10: If $N = 2^n$, $\forall y \in \mathbb{Z}_N$ can be represented by a vector $(x_0, x_1, \ldots, x_{n-1})$ where $y = \sum_{i=0}^{n-1} x_i \cdot 2^i$ for $x_i \in \mathbb{Z}_2$. Let $x_i(1) = x_i$ and $x_i(0)$ denote the negation of $x_i$, i.e. $x_i(0) = 1 - x_i$. We have

$$\delta_i(y) = \delta_i(x_0, x_1, \ldots, x_{n-1}) = \prod_{v=0}^{n-1} x_i(v),$$

where $i = \sum_{v=0}^{n-1} x_v \cdot 2^v$.

The general function form can be represented by the combination of some “linear” terms and “quadratic” terms, which will be defined below, with respect to the Kronecker-delta functions $\delta_{i}(y_k)$ for $i \in \mathbb{Z}_N$ and $0 \leq k \leq m - 1$.

Definition 11: The $\delta$-linear terms are the linear combinations of $\delta_{i}(y_k)$ over $\mathbb{Z}_q$ for $i \in \mathbb{Z}_N$ and $0 \leq k \leq m - 1$. The collection of the $\delta$-linear terms is denoted by

$$\delta_L(q, N) = \left\{ \sum_{k=0}^{m-1} \sum_{i=0}^{N-1} c_{k,i} \delta_{i}(y_k) \bigg| \forall c_{k,i} \in \mathbb{Z}_q \right\}.$$  

Let $\delta(y) = (\delta_{i0}(y), \delta_{i1}(y), \ldots, \delta_{iN-1}(y))$ be a vector function from $\mathbb{Z}_N$ to $\mathbb{Z}_q^N$. We denote the transpose of the vector function $\delta(y)$ by $\delta(y)^T$, and denote the permutation of the vector function $\delta(y)$ by

$$\delta_{\chi}(y) = (\delta_{\chi(0)}(y), \delta_{\chi(1)}(y), \ldots, \delta_{\chi(N-1)}(y)),$$

where $\chi$ is a permutation of symbols $\{0, 1, \ldots, N - 1\}$. The $\delta$-quadratic terms are obtained from the phase matrices $\bar{H} \in S^q_R(q, N)$ introduced in Subsection III-C.

Definition 12: The $\delta$-quadratic terms are quadratic forms:

$$\delta_{\chi_L}(y_0)\bar{H}\delta_{\chi_R}(y_1)^T,$$

where $\chi_L, \chi_R$ are permutations of symbols $\{0, 1, \ldots, N - 1\}$ and $\bar{H} \in S^q_R(q, N)$. The collection of the $\delta$-quadratic terms is denoted by $\delta_Q(q, N)$.

Theorem 3: All the functions extracted from the seed PU matrices can be represented in a general form

$$f(y) = \sum_{k=1}^{m-1} h_k(y_k-1, y_k) + l(y),$$

where $h_k(\cdot) \in \delta_Q(q, N)$ (1 \leq k \leq m - 1) and $l(y) \in \delta_Q(q, N)$.

Theorem 4: The entries of the corresponding function matrix of the seed PU matrix $M(z)$ in (19) at position $(i, j)$ (0 \leq i, j < N) can be expressed by

$$f_{i,j}(y) = f(y) + h(i, y_0) + h'(y_{m-1}, j),$$

where $f(y)$ is a function with the form (26) and $h(\cdot), h'(\cdot) \in \delta_Q(q, N)$.

D. The Proofs of Theorems 3 and 4

From Lemma 2 and formula (22), we have

$$\omega^{f_{i,j}(y)} = H_{i,y_0}^{(0)} \prod_{k=1}^{m-1} H_{y_k-1, y_k}^{(k)} \cdot H_{y_{m-1}, j}^{(m)}.$$  

Let $\bar{H}^{(k)}$ be the phase matrix of the BH matrix $H^{(k)}$ for 0 \leq k \leq m. The function $f_{i,j}(y)$ can be written in the following way.

$$f_{i,j}(y) = \bar{H}_{i,y_0}^{(0)} + \sum_{k=1}^{m-1} \bar{H}_{y_k-1, y_k}^{(k)} + \bar{H}_{y_{m-1}, j}^{(m)}.$$  

If we denote $y_{-1} = i$ and $y_m = j$ for convenience, the above equation can be re-expressed in a unified form:

$$f_{i,j}(y) = \sum_{k=0}^{m} \bar{H}_{y_k-1, y_k}^{(k)}.$$  

Lemma 3: Let $\bar{H}_{y_0, y_n}$ be the entry of $\bar{H}$ at $(y_0, y_n)$, and $h(y_0, y_n)$ a function from $\mathbb{Z}_N^2$ to $\mathbb{Z}_q$ such that

$$h(y_0, y_n) = \bar{H}_{y_0, y_n}.$$

Then $h(y_0, y_n)$ can be represented by the following form:

$$h(y_0, y_n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \bar{H}_{i,j} \delta_{i}(y_0)\delta_{j}(y_n).$$

Proof: Recall the definition of Kronecker-delta functions $\delta_i$ in Definition 10. It follows from $\delta_i(y_0) = \delta_j(y_n) = 1 \iff y_0 = i$ and $y_n = j$.

The function $h(y_0, y_n)$ in (30) can be represented as a matrix form:

$$h(y_0, y_n) = \delta(y_0)\bar{H}\delta(y_n)^T.$$  


According to Lemma 3 and formulas (29) and (31), we obtain a formula for function $f_{i,j}(y)$.

**Lemma 4:** The function $f_{i,j}(y)$ can be expressed in the form:

$$f_{i,j}(y) = \sum_{k=0}^{m} \delta(y_{k-1}) \tilde{H}^{(k)} \delta(y_k)^T.$$  \hspace{1cm} (32)

It seems that we have already obtained the function $f_{i,j}(y)$ from $m + 1$ given phase matrices $\tilde{H}^{(k)}$. However, each phase matrix can be randomly chosen from $H(q, N)$ which is a large set. To obtain a general form of $f_{i,j}(y)$, we take the equivalence of phase matrices into our consideration.

**Lemma 5:** Assume that $Q_1 = \text{diag}\{\omega^{c_0}, \omega^{c_1}, \cdots, \omega^{c_{N-1}}\}$ and $Q_2 = \text{diag}\{\omega^{d_0}, \omega^{d_1}, \cdots, \omega^{d_{N-1}}\}$, $H_1 = Q_1 Q_2$ for $H, H_1 \in H(q, N)$, and $\tilde{H}, \tilde{H}_1$ are the phase matrices of $H$ and $H_1$, respectively. We have

$$\delta(y_0) \tilde{H}_1 \delta(y_N)^T = \delta(y_0) \tilde{H} \delta(y_N)^T + \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} c_i \tilde{d}_i(y_0) \delta_j(y_N).$$

**Proof:** From the definition, we know the entry

$$\{\tilde{H}_1\}_{i,j} = \{\tilde{H}\}_{i,j} + c_i + d_j.$$

Thus

$$\delta(y_0) \tilde{H}_1 \delta(y_N)^T = \delta(y_0) \tilde{H} \delta(y_N)^T + \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} (c_i + d_j) \delta_i(y_0) \delta_j(y_N).$$

**Corollary 1:** The functions extracted from the seed PU matrices can be represented by a general form:

$$f(y) = \sum_{k=1}^{m} \delta_{\chi_{L_k}}(y_{k-1}) \tilde{H}^{(k)} \delta_{\chi_{R_k}}(y_k)^T + \sum_{k=0}^{m-1} \sum_{i=0}^{N-1} c_{k,i} \delta_i(y_k),$$  \hspace{1cm} (33)

where $\chi_{L_k}$ and $\chi_{R_k}$ are both permutations of symbols $\{0, 1, \cdots, N-1\}$, $H^{(k)} \in S_{P_k}(q, N)$ for $1 \leq k \leq m - 1$, and $c_{k,i} \in \mathbb{Z}_q$ for $0 \leq k < m$, $0 \leq i \leq N - 1$.

**Proof:** It is straightforward that $\sum_{i=0}^{N-1} c_i \delta_i(y_i)$ is still a linear combination of the functions $\delta_i(y)$. According to Lemmas 5 and 6, the functions extracted from the seed PU matrices can be expressed in a general form:

$$f(y) = \sum_{k=0}^{m} \delta_{\chi_{L_k}}(y_{k-1}) \tilde{H}^{(k)} \delta_{\chi_{R_k}}(y_k)^T + \sum_{k=0}^{m-1} \sum_{i=0}^{N-1} c_{k,i} \delta_i(y_k),$$  \hspace{1cm} (34)

where $y_{-1} = i$, $y_m = j$. However, for the case $k = 0$ in the first term of the above formula, we have

$$\delta_{\chi_{L,k}}(y_{-1}) \tilde{H} \delta_{\chi_{R,k}}(y_0)^T = \sum_{i=0}^{N-1} c_i \delta_i(y_0),$$

which is a linear combination of $\delta_i(y_0)$. Similarly, for the case $k = m$ in (34), it is still a linear combination of $\delta_i(y_{m-1})$. Then formula (33) is obtained from formula (34).

Theorem 3 follows immediately from Corollary 1 and Definition 12. And Theorem 4 follows from Lemma 4 and Theorem 3.

**E. Function-Based Constructions and Enumerations**

We first study the algebraic structure of the sets $\delta_L(q, N)$ in Definition 11 and $\delta_Q(q, N)$ in Definition 12 to avoid the duplication for the functions with the form (26) in Theorem 3.

An alternative terminology to easily understand the notations and the results in this section is group ring and module theory [43]. Let $(G, \cdot)$ be a semi-group and $\mathbb{Z}_q$ a ring. The semigroup ring of $G$ over $\mathbb{Z}_q$, denoted by $\mathbb{Z}_q[G]$, is the set of mappings $f : G \rightarrow \mathbb{Z}_q$. Furthermore, $\mathbb{Z}_q[G]$ is a $\mathbb{Z}_q$-module. In this subsection, the semi-group $(G, \cdot)$ can be replaced by $(\mathbb{Z}_q^N, \cdot)$ where the operator $\cdot$ denotes element-wise multiplication. Treat 1 as the identity element in $\mathbb{Z}_q[G]$, i.e., the function $1 : G \rightarrow \mathbb{Z}_q$.

From the definition of Kronecker-delta functions $\delta_i$ and the formula $\sum_{i=0}^{N-1} \delta_i = 1$, the algebraic structure of the $\delta_L(q, N)$ is given immediately.
Lemma 7: $\delta_L(q,N)$ is a free $\mathbb{Z}_q$-submodule of dimension $m(N - 1) + 1$ with basis \{\(\delta_i(y_k)\)\(0 \leq k \leq m - 1, 1 \leq i \leq N - 1\) \cup \{1\}. In other word, every $\delta$-linear term is a linear combination of the terms $\delta_i(y_k)$ and 1 over $\mathbb{Z}_q$ for $0 \leq k \leq m - 1$, $1 \leq i \leq N - 1$, so $\delta_L(q,N)$ can be alternatively given by

$$\delta_L(q,N) = \left\{ \begin{array}{l} \sum_{k=0}^{m-1} \sum_{i=1}^{N-1} c_{k,i} \delta_i(y_k) + c', \quad c_{k,i}, c' \in \mathbb{Z}_q, \\ 0 \leq k \leq m - 1, 1 \leq i \leq N - 1 \end{array} \right\}. \quad (35)$$

The number of the $\delta$-linear terms is given by

$$|\delta_L(q,N)| = q^{N(m - m + 1)}.$$

Definition 13: For $h_1(y_0,y_1), h_2(y_0,y_1) \in \delta_Q(q,N)$, we say that $h_1(y_0,y_1)$ and $h_2(y_0,y_1)$ are $\delta$-equivalent if their difference is a $\delta$-linear term. Otherwise, they are called $\delta$-distinct quadratic terms. Let $\delta'_Q(q,N)$ be a subset of $\delta_L(q,N)$ consisting of all the representatives of the functions in $\delta_Q(q,N)$ with respect to this equivalence relation.

Remark 3: Theorems 3 and 4 are still valid if we replace the set $\delta_Q(q,N)$ by the subset $\delta'_Q(q,N)$, since the difference of the $\delta$-equivalent quadratic terms must lie in the set $\delta_L(q,N)$.

Hence all the functions extracted from the seed PU matrices can be represented in a general form

$$f(y) = \sum_{k=1}^{m-1} h_k(y_{k-1}, y_k) + l(y), \quad (36)$$

where $h_k(\cdot, \cdot) \in \delta'_Q(q,N)$ (1 $\leq k \leq m - 1$) and $l(y) \in \delta_L(q,N)$.

We now consider the enumeration of the functions with the form (36), which is obviously a union of the cosets of $\delta_L(q,N)$. Denote the quotient element of $f \in \mathbb{Z}_q[G]$ in the quotient module, $\mathbb{Z}_q[G]$ modulo $\delta_L(q,N)$, by $\overline{f}$. Clearly the number of the functions in (36) are determined by the product of the number of the coset representatives and the cardinality of the set $\delta_L(q,N)$.

Property 3: Properties of $\delta$-distinct quadratic terms in $S'_Q(q,N)$ are listed as follows.

1. $\forall h \in S'_Q(q,N)$, we have $h \notin \delta_L(q,N)$, i.e., $\overline{h} \neq \overline{0}$.
2. $\forall h \in S'_Q(q,N)$, we have $h(0, y_1), h(y_0, 0) \in \delta_L(q,N)$, i.e., $\overline{h}(0, y_1) = \overline{h}(y_0, 0) = \overline{0}$.
3. $\forall h, h' \in S'_Q(q,N)$, we have $h = h' \iff \overline{h} = \overline{h'}$.
4. $\forall h \in S'_Q(q,N)$, there exists a unique $h' \in S'_Q(q,N)$ such that $\overline{h}(y_0, y_1) = \overline{h'}(y_0, y_1)$.

Proof: The properties (1)-(3) directly come from the definition. We only need to prove the properties (4) here. Assume that $h(y_0, y_1) = \delta_{\chi_L(y_0)} H \delta_{\chi_R(y_1)}^T$ for permutations $\chi_L, \chi_R$ and BH matrix $H$. The transpose of $H$ (denoted by $H^T$) is still a BH matrix. Then we have $h(y_1, y_0) \in \delta_Q(q,N)$ by

$$h(y_1, y_0) = \delta_{\chi_L(y_1)} H \delta_{\chi_R(y_0)}^T = \delta_{\chi_R(y_0)} H^T \delta_{\chi_L(y_1)}^T.$$

The existence is proved by letting $h'(y_0, y_1)$ be the representative of $h(y_1, y_0)$ (modulo $\delta_L(q,N)$) in $\delta'_Q(q,N)$.

Each coset representative with the form

$$\sum_{k=1}^{m-1} h_k(y_{k-1}, y_k)$$

uniqueness follows immediately from the definition of the set $\delta'_Q(q,N)$.

Corollary 2: Formula (36) determines $|\delta'_Q(q,N)| = q^{m-1} + q^{Nm-m+1}$ different functions, where $|\delta'_Q(q,N)|$ denotes the number of the functions in the set $\delta'_Q(q,N)$.

Proof: Let $f$ and $f'$ be two coset representatives with the forms

$$f(y) = \sum_{k=1}^{m-1} h_k(y_{k-1}, y_k)$$

and

$$f'(y) = \sum_{k=1}^{m-1} h'_k(y_{k-1}, y_k).$$

We have $\overline{f} = \overline{f'}$, if and only if

$$\sum_{k=1}^{m-1} h_k(y_{k-1}, y_k) = \sum_{k=1}^{m-1} h'_k(y_{k-1}, y_k),$$

if and only if $\overline{h}_k = \overline{h'}_k$ (1 $\leq k \leq m - 1$) by setting $y_\theta = 0$ for $\theta \neq k - 1, k$ (according to Property 3-(2)), if and only if $h_k = h'_k$ (1 $\leq k \leq m - 1$) (according to Property 3-(3)). So different choice of $\{h_k\}_{1 \leq k \leq m - 1}$ leads to different coset representatives, and the number of the coset representatives is $|\delta'_Q(q,N)| = q^{m-1}.$

By applying Theorem 1 in Section III and Theorem 4, we obtain the following results immediately.

Theorem 5: Let $f(y)$ be a function with the form (36) and $h(\cdot, \cdot), h'(\cdot, \cdot) \in \delta'_Q(q,N)$.

1. The following arrays form a CCA of size $N$:

$$f_{i,j}(y) = h(i, y_0) + h'(y_{m-1}, j), \quad 0 \leq i, j < N.$$

2. For any $\pi$, the sequences evaluated by following functions form a CCC of size $N$:

$$\pi \cdot f_{i,j}(y) = f_{i,j}(y_{\pi(0)}, y_{\pi(1)}, \ldots, y_{\pi(m-1)}), \quad 0 \leq i, j < N.$$

3. The following arrays form a CAS of size $N$:

$$f_i(y) = f(y) + h(i, y_0), \quad 0 \leq i < N.$$

4. For any $\pi$, the $q$-ary sequences evaluated by following functions form a CSS of size $N$ and length $N^m$:

$$\pi \cdot f_i(y) = f_i(y_{\pi(0)}, y_{\pi(1)}, \ldots, y_{\pi(m-1)}), \quad 0 \leq i < N.$$

We denote a set consisting of all the sequences in the CSSs constructed in Theorem 5 by $S(q,N)$. Since the set $\delta_L(q,N)$ is an invariant under any permutation of variables $y$, $S(q,N)$ is a union of the cosets of $\delta_L(q,N)$, i.e.,

$$S(q,N) = \left\{ \sum_{k=1}^{m-1} h_k(y_{\pi(k-1)}, y_{\pi(k)}) + l(y) \right\}$$

$$h_k(\cdot, \cdot) \in \delta'_Q(q,N), \quad l(y) \in \delta_L(q,N). \quad (37)$$

Each coset representative with the form

$$\sum_{k=1}^{m-1} h_k(y_{\pi(k-1)}, y_{\pi(k)})$$

(38)
can be associated with a directed and weighted Hamilton path on \( m \) vertices as shown in Figure 2, where we label the vertices of the coset representative by \( y_0(0), y_1(1), \ldots, y_{m-1}(m-1) \) and join vertices \( y_{\pi(k-1)} \) and \( y_{\pi(k)} \) by a directed edge labeled \( h_k(\cdot, \cdot) \).

**Remark 4:** For a given coset representative with the form (38), its corresponding directed and weighted Hamilton path shown in Figure 2 may be not unique. Vertices \( y_0 \) and \( y_k \) are adjacent if and only if formula (38) modulo \( \delta_L(q, N) \) does not equal \( \theta \) by setting \( y_k = 0 \) for \( k \neq \theta, \eta \). Then the neighbors of \( y_\pi(k) \) must be \( y_{\pi(k-1)} \) and \( y_{\pi(k+1)} \), and the endpoints (who has only one neighbor) must be \( y_{\pi(0)} \) and \( y_{\pi(m-1)} \). Thus, the directed Hamilton path of representative with the from (38), must be labeled in the order \( y_{\pi(0)}; y_{\pi(1)}; \ldots; y_{\pi(m-1)} \) or in the reverse order \( y_{\pi(m-1)}; y_{\pi(m-2)}; \ldots; y_{\pi(1)}; y_{\pi(0)} \).

**Corollary 3:** The set \( S(q, N) \) determines exactly

\[
\frac{1}{2} m! \cdot |\delta_L(q, N)|^{m-1} \cdot q^{Nm-m+1}
\]

different sequences.

**Proof:** Let \( \pi \cdot f(y) \) and \( \pi' \cdot f'(y) \) be two coset representatives where

\[
f(y) = \sum_{k=1}^{m-1} h_k(y_{k-1}, y_k)
\]

and

\[
f'(y) = \sum_{k=1}^{m-1} h'_k(y_{k-1}, y_k).
\]

If \( \pi \cdot f = \pi' \cdot f' \), i.e.,

\[
\sum_{k=1}^{m-1} \overline{h}_k(y_{\pi(k-1)}, y_{\pi(k)}) = \sum_{k=1}^{m-1} \overline{h}'_k(y_{\pi'(k-1)}, y_{\pi'(k)}),
\]

we have \( \pi = \pi' \) or \( \pi(k) = \pi'(m-k) \) for \( 1 \leq k \leq m-1 \) by Remark 4.

For the first case \( \pi = \pi' \), the condition \( \pi \cdot f = \pi' \cdot f' \) leads to \( h_k = h'_k \) for \( 1 \leq k \leq m-1 \) by a similar argument in the proof of Corollary 2.

For the second case \( \pi(k) = \pi'(m-k) \), according to Property 3-(2), the condition \( \pi \cdot f = \pi' \cdot f' \) leads to \( \overline{h}(y_{\pi(k-1)}, y_{\pi(k)}) = \overline{h}'(y_{\pi'(k-1)}, y_{\pi'(k)}) \) \((1 \leq k \leq m-1)\) by setting \( y_0 = 0 \) for \( \theta \neq \pi(k-1), \pi(k) \). From Property 3-(4), for each \( h_k \), there exists a unique \( h'_{m-k} \in S'(q, N) \) such that

\[
\overline{h}(y_{0}, y_1) = \overline{h}'_{m-k}(y_1, y_0).
\]

Thus, \( \pi \cdot f = \pi' \cdot f' \) if and only if

1. \( \pi(k) = \pi'(k), h_k(y_0, y_1) = h'_k(y_0, y_1) \) for \( 1 \leq k \leq m-1 \);
2. \( \pi(k) = \pi'(m-k), h_k(y_0, y_1) = h'_k(y_0, y_1) \) for \( 1 \leq k \leq m-1 \).

From the discussion above, for a given pair \((f(y), \pi)\), there exists a unique pair \((f'(y), \pi') \neq (f(y), \pi)\), which is determined by the case (2) in the above conditions, such that \( \pi \cdot f(y) = \pi' \cdot f'(y) \). Thus, the number of the sequences in set \( S(q, N) \) is equal to half of the product of the number of the permutations and the number of the functions in (36).

**Remark 5:** As shown in Remark 2, the PU matrices proposed in [9] can be treated as the sequence version of the seed PU matrices proposed in this paper, so the enumeration of the sequences here and [9] should be identical. However, [9, Section VI] showed that there are \( m! \cdot (\frac{N!}{n_0}) \cdot q^{Nm-n_0} \) different sequences, where \( n_0 \) is a specified number. For example, for the case \( N = 2 \) and the case \( N = q = 3 \), \( n_0 \) in [9] equals to Euler function \( \varphi(N) \). For the case \( N = 2 \), Corollary 3 in this paper determines \( m! \cdot q^{m+1} \) Golay sequences, whereas there are \( m! \cdot q^{m+1} \) in [9]. For the case \( N = q = 3 \), Corollary 3 determines \( m! \cdot 2m^2 \cdot 3^{2m+1} \) ternary sequences, whereas there are \( m! \cdot 2m^2 \cdot 3^{2m+1} \) in [9]. A general explicit form of the functions constructed here will be given in Subsections V-B and V-C for the cases of \( N = 2 \) and \( N = q = 3 \) respectively, which both agree with the enumeration in this paper. Thus, the results in Corollary 3 directly from functions correct the enumeration in [9] from PU matrices.

V. Parameterized Constructions from Seed PU Matrices

From the discussions in Subsection IV-E, we need two ingredients, the set \( \delta_L(q, N) \) and \( \delta_Q(q, N) \), to calculate the explicit form of functions (or sequences) for given \( q \) and \( N \). The detailed processes are shown as follows.

1. Determine the set \( S_H(q, N) \), which consists of all the representatives of phase matrices in \( \tilde{H}(q, N) \).
2. Find the functions \( \delta_i : \mathbb{Z}_N \to \mathbb{Z}_q \) such that \( \delta_i(j) = \delta_{i,j} \) for \( i, j \in \mathbb{Z}_N \). Then compute the set

\[
\delta_L(q, N) = \left\{ \sum_{k=0}^{m-1} \sum_{i=1}^{N-1} c_{k,i} \delta_i(y_k) + c' \middle| c_{k,i}, c' \in \mathbb{Z}_q, \right. 0 \leq k \leq m-1, 1 \leq i \leq N-1 \right\}.
\]

3. Compute the bivariate functions by \( \delta_{XL}(y_0) \tilde{H} \delta_{XR}(y_1)^T \), \forall \tilde{H} \in S_H(q, N) \) and \( \forall \delta_{XL}, \delta_{XR} \) the permutations of symbols \( \{0, 1, \ldots, N-1\} \). The set \( \delta_Q(q, N) \) is obtained by collecting all the representatives of the functions of the form \( \delta_{XL}(y_0) \tilde{H} \delta_{XR}(y_1)^T \) with respect to \( \delta_L(q, N) \).

4. Any function extracted from the seed PU matrices can be expressed in a general form

\[
f = \sum_{k=1}^{m-1} h_k(y_{k-1}, y_k) + \delta_L(q, N),
\]

where \( h_k(\cdot, \cdot) \in \delta'_L(q, N) \) for \( 1 \leq k \leq m-1 \).

5. CCAs, CASs, CCCs and CSSs are constructed by Theorem 5.

For Step (1), there is a large volume of the research papers on the existences, enumerations and constructions of the BH matrices. A source of BH matrices with small \( N \) and \( q \) can be found in [30]. We will see from the following subsections that the computations on Step (3) is heavy. It is obvious that Steps (4) and (5) are straightforward if Steps (2) and (3) are established. We give the cases for \( N = 2 \) and \( q \) even, \( N = q = 3 \), and \( N = 4 \), \( q = 2 \) or \( 4 \) in the rest of the four subsections.
A. Case \( N = 2 \): Golay Sequences

From Example 4, BH matrices of order 2 do not exist for \( q \) odd. Let \( N = 2 \) and \( q \) even.

(1) Determine the set \( S_{\Pi}_F(q, 2) \). From Example 7, there is only one phase matrix in \( S_{\Pi}_F(q, 2) \):

\[
\begin{bmatrix}
0 & 0 \\
0 & q/2
\end{bmatrix}.
\]

(2) Computation of the set \( \delta_L(q, 2) \). From Example 10, we have the basis functions

\[
\begin{aligned}
\delta_0(x) &= 1 - x, \\
\delta_1(x) &= x.
\end{aligned}
\]

Then we obtain the \( \delta \)-linear terms

\[
\delta_L(q, 2) = \left\{ \sum_{k=0}^{m-1} c_k x_k + c', \quad c_k, c' \in \mathbb{Z}_q, 0 \leq k \leq m - 1 \right\}.
\]

(3) Computation of the set \( \delta'_L(q, 2) \). We have

\[
\delta(x) = (\delta_0(x), \delta_1(x)) = (1 - x, x) = (-1, 1)x + (0, 1) \cdot 1.
\]

The term \( (1, 0) \cdot 1 \) only produces the \( \delta \)-linear terms in \( \delta_{xL}(x_0)H \delta_{xR}(x_1) \). So we only need to consider the term \( \delta'(x) = (-1, 1)x \). Let \( \chi \) be a permutation of symbols \( \{0, 1\} \).

Then \( \delta'_L(x) = (-1, 1)x \) or \( \delta'_L(x) = (1, -1)x \). For any permutations \( \chi_L \) and \( \chi_R \), we have

\[
\begin{aligned}
\delta'_L(x_0) &= 0 \\
\delta'_L(x_1) &= q/2,
\end{aligned}
\]

\[
\chi_L(-1, 1) = \begin{bmatrix} 0 & 0 \\ q/2 & 0 \end{bmatrix},
\]

\[
\chi_R(-1, 1) = \begin{bmatrix} q/2 & 0 \\ 0 & q/2 \end{bmatrix}.
\]

So \( \delta'_L(q, 2) \) contains only one function: \( \chi_{\delta}x_{0, x_1} \).

By applying Theorem 5, we obtain the following construction.

Construction 1: Let \( \pi \) be a permutation of \( \{0, 1, \ldots, m - 1\} \). For \( N = 2 \) and \( q \) even, we have

(1) The Golay arrays extracted from the seed PU matrices can be expressed by

\[
f(x_0, x_1, \ldots, x_{m-1}) = \frac{q}{2} \sum_{k=0}^{m-1} x_{k-1}x_k + \sum_{k=0}^{m-1} c_k x_k + c',
\]

(39)

for \( c_k, c' \in \mathbb{Z}_q, 0 \leq k \leq m - 1 \).

(2) The corresponding function matrix \( \widetilde{M}(x) \) is given by

\[
\widetilde{M}(x) = f \cdot J_2 + \frac{q}{2} \begin{bmatrix} 0 & x_{m-1} \\ x_0 & x_0 + x_{m-1} \end{bmatrix},
\]

where the GBF \( f \) is in the form (39). The sequences evaluated by the matrix \( \pi \cdot \widetilde{M}(x) \) form aCCC of size 2.

(3) The set \( S(q, 2) \) consisting of all the Golay sequences derived from the seed PU matrices of order 2 is given by

\[
S(q, 2) = \left\{ \frac{q}{2} \sum_{k=0}^{m-1} x_{(k-1) \Delta \pi, (k) \Delta \pi} + \sum_{k=0}^{m-1} c_k x_k + c' \right\}
\]

\[
\forall \pi, \forall c_k, c' \in \mathbb{Z}_q, 0 \leq k < m - 1 \}
\]

(4) The sequences evaluated by

\[
\begin{aligned}
f, \\
\frac{f + q}{2} x_{\pi(0)}
\end{aligned}
\]

form a GSP for \( f \in S(q, 2) \).

This construction coincides with the well known results on standard Golay sequences [10] by Davis and Jedwab. The enumeration in Corollary 3 for \( N = 2 \) also agrees with the number of the standard Golay sequences.

B. Case \( N = q = 3 \): Ternary Sequences of Size 3

Let \( N = q = 3 \) in this subsection.

(1) Determine the set \( S_{\Pi}_F(3, 3) \). There is only one phase matrix in \( H(3, 3) \):

\[
\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}.
\]

(2) Computation of the set \( \delta_L(3, 3) \). From Definition 10, it is easy to verify that

\[
\begin{aligned}
\delta_0(y) &= 2y^2 + 1, \\
\delta_1(y) &= 2y^2 + 2y, \\
\delta_2(y) &= 2y^2 + y.
\end{aligned}
\]

Then we obtain the \( \delta \)-linear terms

\[
\delta_L(3, 3) = \left\{ \sum_{k=0}^{m-1} c_{k, 2} y_k^2 + \sum_{k=0}^{m-1} c_{k, 1} y_k + c' \right\} c_{k, 1}, c_{k, 2}, c' \in \mathbb{Z}_3, 0 \leq k \leq m - 1 \}
\]

(3) Computation of the set \( \delta'_L(3, 3) \). We have

\[
\delta(y) = (\delta_0(y), \delta_1(y), \delta_2(y)) = (2y^2 + 1, 2y^2 + 2y, 2y^2 + y) = (2, 2, 2)y^2 + (0, 2, 1)y + (1, 0, 0) \cdot 1.
\]

The term \( (1, 0, 0) \cdot 1 \) only produces the \( \delta \)-linear terms in \( \delta_{xL}(y_0)H \delta_{xR}(y_1) \). So we only need to consider

\[
\delta'(y) = (2, 2, 2)y^2 + (0, 2, 1)y
\]

and

\[
\delta'_L(y) = (2, 2, 2)y^2 + ey,
\]
where
e \in E = \{(0, 2, 1), (0, 1, 2), (1, 0, 2), (1, 2, 0), (2, 1, 0), (2, 0, 1)\}.

For any permutations \(\chi_L\) and \(\chi_R\) of \(\{0, 1, 2\}\), we have
\[
\begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 2 \\
0 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 2 \\
0 & 2 & 1
\end{bmatrix}
= \begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 2 \\
0 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 2 \\
0 & 2 & 1
\end{bmatrix}
= (2, 2, 2)^T y_0^2 + e_1 y_0,
\]
where \(e_1, e_2 \in E\). Since
\[
(2, 2, 2)^T y_0^2 + e_1 y_0 = (0, 0, 0)^T,
\]
we have
\[
\begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 2 \\
0 & 2 & 1
\end{bmatrix}
\begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 2 \\
0 & 2 & 1
\end{bmatrix}
= (0, 0, 0)^T,
\]
By substituting the vectors \(e_1, e_2 \in E\) into the above formula, we obtain
\[
\delta_Q(3, 3) = \{y_0 y_1, 2 y_0 y_1\}.
\]
By applying Theorem 5, we obtain the following construction. 

Construction 2: Let \(\pi\) be a permutation of \(\{0, 1, \cdots, m - 1\}\). For \(N = q = 3\), we have

(1) The ternary arrays extracted from the seed PU matrices can be expressed by
\[
f(y_0, y_1, \cdots, y_{m-1}) = \sum_{k=1}^{m-1} d_k y_{k-1} y_k + \sum_{k=0}^{m-1} c_k y_k + c',
\]
for \(d_k \in \mathbb{Z}_3^+ (1 \leq k < m)\), \(c_{k,1}, c_{k,2}, c' \in \mathbb{Z}_3 (0 \leq k < m)\).

(2) The corresponding function matrix \(\overline{M}(y)\) is given by
\[
\overline{M}(y) = f \cdot J_3 + \begin{bmatrix}
0 & y_0 & y_0 \\
y_0 & y_0 + y_{m-1} & y_0 + y_{m-1} \\
y_0 & y_0 + y_{m-1} & y_0 + y_{m-1}
\end{bmatrix},
\]
where the function \(f\) is in the form (40).

(3) The collection of ternary sequences in CSSs of size 3 derived from the seed PU matrices of order 3 can be expressed by
\[
S(3, 3) = \left\{ \sum_{k=1}^{m-1} d_k y_{\pi(k-1)} y_{\pi(k)} + \sum_{k=0}^{m-1} c_k y_k^2 + \sum_{k=0}^{m-1} c_{k,1} y_k + c' \right\},
\]
for \(\forall \pi, \forall d_k \in \mathbb{Z}_3^+ (1 \leq k < m)\), \(\forall c_{k,1}, c_{k,2}, c' \in \mathbb{Z}_3 (0 \leq k < m)\).

(3) The sequences evaluated by
\[
\delta(y) = (\delta_0(y), \delta_1(y), \delta_2(y), \delta_3(y))
\]
form a ternary CSS of size 3 for \(f \in S(3, 3)\).

From the enumeration in Corollary 3, the set \(S(3, 3)\) determines exactly \(m! \cdot 2^{m-2} \cdot 3^{2m+1}\) sequences for \(m > 1\). As far as our knowledge, the sequences in Construction 2 are never reported in the literature.

C. Case \(N = 4\) and \(q = 2\): Binary Sequences of Size 4
Let \(N = 4, q = 2\) in this subsection.

(1) Determine the set \(S_H(2, 4)\). From Example 8, there is only one phase matrix in \(S_H(2, 4)\):
\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0
\end{bmatrix}.
\]

(2) Computation of the set \(\delta_L(2, 4)\). From the proof in the Subsection IV-C, if we take the direct product of two \(\mathbb{Z}_2\) to replace \(\mathbb{Z}_4\), the results are still valid. So any variable \(y \in \mathbb{Z}_4\) can be represented by \((x_0, x_1)\), where \(y = 2x_1 + x_0\) and \(x_0, x_1 \in \mathbb{Z}_2\). From Example 10, we have the basis functions
\[
\delta_0(y) = (1 - x_0)(1 - x_1),
\delta_1(y) = x_0(1 - x_1),
\delta_2(y) = (1 - x_0)x_1,
\delta_3(y) = x_0x_1.
\]

Let \(y_k = (x_{2k}, x_{2k+1})\). Then the function \(f(y_0, y_1, \cdots, y_{2m-1})\) can be re-expressed by a GBF
\[
f(x_0, x_1, \cdots, x_{2m-1}).
\]

The \(\delta\)-linear terms are given by
\[
\delta_L(2, 4) = \left\{ \sum_{k=0}^{m-1} d_k x_{2k} x_{2k+1} + \sum_{k=0}^{2m-1} c_k x_k + c' \right\}
\]
for \(\forall d_k, c_k, c' \in \mathbb{Z}_2, 0 \leq k \leq 2m - 1\).

(3) Computation of the set \(\delta_Q(2, 4)\). We have
\[
\delta(y) = (\delta_0(y), \delta_1(y), \delta_2(y), \delta_3(y))
\]
where
\[
\delta_0(y) = (1, -1, -1, 1)x_0x_1 + (-1, 1, 0, 0)x_0 + (-1, 0, 1, 0)x_1 + (1, 0, 0, 0),
\]
It is obvious that \((1, 0, 0, 0, \cdots)\) only produces \(\delta\)-linear terms. For any permutation \(\chi\) of \(\{0, 1, 2, 3\}\), we have
\[
\chi(1, -1, -1, 1) \begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0
\end{bmatrix} = (0, 0, 0, 0).
\]
and
\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 \\
\end{bmatrix}
\begin{bmatrix}
1 \\
-1 \\
-1 \\
1 \\
\end{bmatrix}
= (0, 0, 0, 0)^T.
\]

So we only need to consider
\[
\delta'_\chi(y) = \chi(-1, 1, 0, 0)x_0 + \chi(-1, 0, 1, 0)x_1
= \chi(-x_1 - x_0, x_0, x_1, 0).
\]

By computing
\[
S = \delta'_{\chi_L}(y_0) = \begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 \\
\end{bmatrix}
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 \\
\end{bmatrix}
= \chi_L(-x_1 - x_0, x_0, x_1, 0)
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 \\
\end{bmatrix}
\chi_R(-x_3 - x_2)
\begin{bmatrix}
x_2 \\
x_3 \\
0 \\
0 \\
\end{bmatrix}
\]

for all permutation \(\chi_L, \chi_R\) of \(\{0, 1, 2, 3\}\), we obtain the set
\[
\delta'_Q(2, 4) = \{\varphi_i((x_0, x_1), (x_2, x_3)) \mid 1 \leq i \leq 6\},
\]

where
\[
\begin{align*}
\varphi_1 &= x_0 x_2 + x_0 x_3 + x_1 x_2, \\
\varphi_2 &= x_0 x_2 + x_0 x_3 + x_1 x_3, \\
\varphi_3 &= x_0 x_2 + x_1 x_3 + x_1 x_2, \\
\varphi_4 &= x_1 x_3 + x_0 x_3 + x_1 x_2, \\
\varphi_5 &= x_0 x_3 + x_1 x_2, \\
\varphi_6 &= x_1 x_3 + x_0 x_2.
\end{align*}
\]

By applying Theorem 5, we obtain the following construction.

**Construction 3:** Let \(\pi\) be a permutation of \(\{0, 1, \ldots, m-1\}\) and \(x = (x_0, x_1, \ldots x_{2m-1})\). For \(N = 4\) and \(q = 2\), we have

1. The binary arrays extracted from the seed PU matrices can be expressed by
   \[
   f(x) = \sum_{k=1}^{m-1} h_k((x_2k-2, x_{2k-1}), (x_2k, x_{2k+1}))
   + \sum_{k=0}^{2m-1} d_k x_{2k} x_{2k+1} + \sum_{k=0}^{2m-1} c_k x_k + c',
   \]
   for \(h_k(\cdot, \cdot) \in \delta'_Q(2, 4)(1 \leq k \leq m-1)\) and \(d_k, c_k, c' \in \mathbb{Z}_2, 0 \leq k \leq m-1\).

2. The corresponding function matrix \(\tilde{M}(x)\) is given by
   \[
   \tilde{M}(x) = f \cdot J_4 + A(x_0, x_1) \cdot J_4 + J_4 \cdot A(x_{2m-2}, x_{2m-1})
   \]
   where the GBF \(f\) is in the form (41) and \(A(x_0, x_1) = diag(0, x_0, x_1, x_0 + x_1)\) is a diagonal matrix.

3. The collection of binary sequences in CSSs of size 4 derived from the seed PU matrices of order 4 can be expressed by
   \[
   S(2, 4) = \left\{ \sum_{k=1}^{m-1} h_k((x_2\pi(k-1), x_2\pi(k-1)+1), (x_2\pi(k)), x_2\pi(k)+1) + \sum_{k=0}^{2m-1} d_k x_{2k} x_{2k+1} + \sum_{k=0}^{2m-1} c_k x_k + c' \right\}
   \]
   for \(h_k(\cdot, \cdot) \in \delta'_Q(2, 4)(1 \leq k \leq m-1)\) and \(d_k, c_k, c' \in \mathbb{Z}_2, 0 \leq k \leq m-1\).

(4) The sequences evaluated by
   \[
   \begin{align*}
   f + x_2 \pi(0), \\
   f + x_2 \pi(0)+1, \\
   f + x_2 \pi(0) + x_2 \pi(0)+1
   \end{align*}
   \]
   form a binary CSS of size 4 for \(f \in S(2, 4)\).

The sequences in Construction 3 can be obtained from the results in [54]. Furthermore, the first-order Reed-Muller code is a sub-code of \(\delta_1(2, 4)\). Note that \(|RM_2(1, 2m)| = 2^{2m+1}\), while \(|\delta_1(2, 4)| = 2^{3m+1}\). The sequences shown here fill up \(\frac{1}{4}m! \cdot 6^{m-1}\) distinct cosets of \(\delta_1(2, 4)\) where the collection of the coset representatives are in the set
\[
\left\{ \sum_{k=1}^{m-1} h_k((x_2\pi(k-1), x_2\pi(k-1)+1), (x_2\pi(k)), x_2\pi(k)+1) \right\}
\]

From the enumeration in Corollary 3, the set \(S(2, 4)\) determines \(m! \cdot 6^{m-1}2^{3m}\) sequences.

**Remark 6:** Note that the size of the arrays extracted here is \(4 \times 4 \times \cdots \times 4\). The number of the variables of GBFs in the form (41) is \(2m\), but \(\pi\) in Construction 3 is a permutation of \(\{0, 1, \ldots, m-1\}\). We will construct the arrays of size \(2 \times 2 \times \cdots \times 2\) and extend the results in Construction 3 in next section.

**D. Case N = 4 and q = 4:** Quaternary Sequences of Size 4

Let \(N = 4, q = 4\) in this subsection.

1. Determine the set \(S_R(4, 4)\). From Example 9, there are two phase matrices in \(S_R(4, 4)\), which are
   \[
   \begin{bmatrix}
   0 & 0 & 0 & 0 \\
   0 & 2 & 0 & 2 \\
   0 & 0 & 2 & 2 \\
   0 & 2 & 2 & 0 \\
   \end{bmatrix}
   \]
   \[
   \begin{bmatrix}
   0 & 0 & 0 & 0 \\
   0 & 1 & 2 & 3 \\
   0 & 2 & 0 & 2 \\
   0 & 3 & 2 & 1 \\
   \end{bmatrix}
   \]

2. Computation of the set \(\delta_1(4, 4)\). The arguments are the same as the case \(\delta_1(2, 4)\). Any variable \(y \in \mathbb{Z}_4\) can be represented by \((x_0, x_1)\) for \(x_0, x_1 \in \mathbb{Z}_2\). From Example 10, we have the basis functions
   \[
   \begin{align*}
   \delta_0(y) &= (1 - x_0)(1 - x_1), \\
   \delta_1(y) &= x_0(1 - x_1), \\
   \delta_2(y) &= (1 - x_0)x_1, \\
   \delta_3(y) &= x_0x_1.
   \end{align*}
   \]


Let $y_k = (x_{2k}, x_{2k+1})$. We obtain the \( \delta \)-linear terms
\[
\delta_L(4, 4) = \left\{ \sum_{k=0}^{m-1} d_k x_{2k} x_{2k+1} + \sum_{k=0}^{2m-1} c_k x_k + c' \right\}
\forall d_k, c_k, c' \in \mathbb{Z}_4, 0 \leq k \leq 2m - 1.
\]
(3) Computation of the set \( \delta'_Q(4, 4) \). Note that the case for the WHT matrix has been studied in the previous subsection. It is known \( \delta'_Q(2, 4) = \{ \varphi_1 \} \). Then \( \{ 2 \varphi_1 \} \), which are derived from the WHT matrix, is a subset of \( \delta'_Q(4, 4) \). So we only need to consider the DFT matrix. We have
\[
\delta(y) = (1, -1, -1, 1)x_0 x_1 + (-1, 1, 0, 0)x_0 + (-1, 0, 1, 0)x_1 + (1, 0, 0, 0) \cdot 1.
\]
The term \((1, 0, 0, 0) \cdot 1\) only produces \( \delta \)-linear terms. So we only consider
\[
\delta'(y) = (1, -1, -1, 1)x_0 x_1 + (-1, 0, 1, 0)x_1 + (-1, 1, 0, 0)x_0.
\]
By computing
\[
\delta'_{\chi_L}(y_0 = (x_0, x_1)) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 3 & 2 & 1 \end{bmatrix} \quad \delta'_{\chi_R}(y_1 = (x_2, x_3))^T
\]
for all permutation \( \chi_L, \chi_R \) of \( \{0, 1, 2, 3\} \), and combining the functions in \( \delta'_Q(2, 4) \), we obtain the set
\[
\delta'_Q(4, 4) = \{ \psi_i((x_0, x_1), (x_2, x_3)) \mid 1 \leq i \leq 9, \quad a_0 \in \{0, 1, 2, 3\}, a_1 \in \{1, 2, 3\}, a_2 \in \{1, 3\} \},
\]
where
\[
\begin{align*}
\psi_1 &= a_0 x_0 x_3 + 2 x_1 x_3 + x_2 x_3, \\
\psi_2 &= a_0 x_1 x_2 + 2 x_0 x_2 + 2 x_1 x_3, \\
\psi_3 &= a_1 x_0 x_3 + 2 x_1 x_3 + x_2 x_3, \\
\psi_4 &= a_1 x_0 x_2 + 2 x_1 x_2 + 2 x_0 x_3, \\
\psi_5 &= a_2 x_1 x_3 + (a + 2) x_0 x_3 + 2 x_1 x_2 + 2 x_0 x_2 + 2 x_0 x_1 x_3, \\
\psi_6 &= a_2 x_1 x_2 + (a + 2) x_0 x_2 + 2 x_1 x_3 + 2 x_0 x_3 + 2 x_0 x_1 x_2, \\
\psi_7 &= a_2 x_1 x_3 + (a + 2) x_0 x_2 + 2 x_0 x_3 + 2 x_0 x_2 + 2 x_1 x_2 x_3, \\
\psi_8 &= a_2 x_0 x_3 + (a + 2) x_0 x_3 + 2 x_1 x_2 + 2 x_1 x_3 + 2 x_0 x_2 x_3, \\
\psi_9 &= a_2 x_0 x_2 + (a + 2) x_0 x_3 + (a + 2) x_1 x_2 + a_2 x_1 x_3 + 2 x_0 x_1 x_2 + 2 x_0 x_2 x_3 + 2 x_1 x_2 x_3.
\end{align*}
\]
By applying Theorems 3 and 5, we obtain the following construction.

Construction 4: Let \( \pi \) be a permutation of \{0, 1, \ldots, m - 1\} and \( \mathbf{x} = (x_0, x_1, \ldots x_{2m-1}) \). For \( N = 4 \) and \( q = 4 \), we have

(1) The quaternary arrays extracted from the seed PU matrices can be expressed by
\[
f(\mathbf{x}) = \sum_{k=1}^{m-1} h_k((x_{2k-2}, x_{2k-1}), (x_{2k}, x_{2k+1})) + \sum_{k=0}^{2m-1} d_k x_{2k} x_{2k+1} + \sum_{k=0}^{2m-1} c_k x_k + c' \quad (42)
\]
for \( h_k(\cdot, \cdot) \in \delta'_Q(4, 4)|1 \leq k \leq m - 1\) and \( d_k, c_k, c' \in \mathbb{Z}_4, 0 \leq k \leq m - 1\).

(2) The computation of quaternary sequences in CSSs of size 4 derived from the seed PU matrices of order 4 is given by
\[
S(4, 4) = \left\{ \sum_{k=1}^{m-1} h_k((x_2 \pi(k-1), x_2 \pi(k-1)+1), (x_2 \pi(k)), x_2 \pi(k+1)) + \sum_{k=0}^{2m-1} d_k x_{2k} x_{2k+1} + \sum_{k=0}^{2m-1} c_k x_k + c' \right\}
\forall h_k(\cdot, \cdot) \in \delta'_Q(4, 4)|1 \leq k \leq m - 1\) and \( d_k, c_k, c' \in \mathbb{Z}_4, 0 \leq k \leq m - 1\).

For the sequences in Construction 4, if \( h_k(\cdot, \cdot) \) are all chosen from the subset \{ \psi_i | 1 \leq i \leq 4 \} in \( \delta'_Q(4, 4) \) for \( 1 \leq k \leq m - 1 \), these sequences have been introduced in [54].

Example 11: Let \( m = 2 \), and \( h_1(\cdot, \cdot) \) is chosen as \( \psi_7 \) with \( a_2 = 1 \), then we have
\[
f_1 = x_1 x_3 + 3 x_0 x_3 + 2 x_1 x_2 + 2 x_0 x_2 + 2 x_0 x_1 x_3.
\]
Let \( m = 2 \), and \( h_1(\cdot, \cdot) \) is chosen as \( \psi_9 \) with \( a_2 = 1 \), we have
\[
f_2 = x_0 x_2 + 2 x_0 x_3 + 3 x_1 x_2 + 2 x_1 x_3 + 2 x_0 x_1 x_3 + 2 x_0 x_2 x_3 + 2 x_1 x_2 x_3.
\]
Each sequence evaluated by the above GBFs lie in a CSS of size 4 respectively.

From Example 11, even for the sequences in CSSs of size 4 and length \( 2^4 \) evaluated by the functions in \{ \psi_i | 1 \leq i \leq 4 \}, they are never reported in the literature, such as [6], [33], [42], [44], [54]. Moreover, for sequence \( f \in S(4, 4) \), if there exists \( k \), such that \( h_k(\cdot, \cdot) \) is chosen from the subset \{ \psi_i | 5 \leq i \leq 9 \}, CSSs of size 4 constructed here must be new, which asserts that the number of the quaternary sequences in CSSs of size 4 can be significantly increased.

The first-order GRM code is a sub-code of \( \delta_L(4, 4) \). Note that \( |RM_k(1, 2m)| = 4^{2m+1} \), while \( |\delta_L(4, 4)| = 4^{3m+1} \). The sequences constructed here fill up \( \frac{1}{24^m} \cdot 24^{m-1} \) cosets of \( \delta_L(4, 4) \) where the collection of the coset representatives are shown in the set
\[
\left\{ \sum_{k=1}^{m-1} h_k((x_2 \pi(k-1), x_2 \pi(k-1)+1), (x_2 \pi(k), x_2 \pi(k+1))) \right\}
\forall h_k(\cdot, \cdot) \in \delta'_Q(4, 4), 1 \leq k \leq m - 1\.
\]
From the enumeration in Corollary 3, the set \( S(4, 4) \) determines exactly \( \frac{1}{24^m} \cdot 24^{m-1} \cdot 4^{3m+1} \) sequences.

For the known complementary sequences with explicit GBFs, quaternary sequences are always generalized from the binary case. Here the sequences in \( S(4, 4) \) are generalized from the binary case if and only if all \( h_k(\cdot, \cdot) \) are chosen from the subset \{ \psi_i | 1 \leq i \leq 4 \} in \( \delta'_Q(4, 4) \). One important reason is that the coset representatives are computed by both WHT matrix and DFT matrix of order 4, which lead to that the number of the coset representatives in \( S(4, 4) \) is \( \frac{1}{24^m} \cdot 24^{m-1} \). On the other hand, for the case that the coset representatives
are only computed by the WHT matrix, the number of the coset representatives in $S(2, 4)$ is $\frac{1}{2} m! \cdot 6^{m-1}$.

**Remark 7:** Similar to Remark 6, we will construct the arrays of size $2 \times 2 \times \cdots \times 2$ and extend the results in Construction 4 in next section.

VI. GENERALIZED SEED PU MATRICES AND CORRESPONDING SEQUENCES

We have shown in Constructions 3 and 4 in Section V that the binary and quaternary sequences in CSSs of size 4 are obtained by action of permutations on the arrays of size $4 \times 4 \times 4 \times \cdots \times 4$. Although these sequences are all evaluated by the GBFs with Boolean variables $(x_0, x_1, \cdots, x_{2m-1})$, we can only permute the variables $(y_0, y_1, \cdots, y_{m-1})$ for $y_k \in \mathbb{Z}_4$ to enlarge the sequence set from the results in previous section. On the other hand, permuting the Boolean variables of the complementary sequences constructed in the literature, such as [10], [33], [42], are still complementary sequences in CSS of the same size. It is natural to ask whether the GBFs extracted from the seed PU matrices of size $N = 2^n$ can represent the complementary arrays of size $2 \times 2 \times \cdots \times 2$.

We set $N = 2^n$ (i.e., $N = p^n$ and $p = 2$) in this section, and construct PU matrices of size $2^n$ and arrays of size $2 \times 2 \times \cdots \times 2$. Then we can apply Theorem 1-(5) in Section III to construct more new CCCs and CSSs.

A. Generalized Seed PU Matrices

For $N = 2^n$, we generalize the delay matrix by the Kronecker product of delay matrix

$$D(z) = \begin{bmatrix} 1 & 0 \\ 0 & z \end{bmatrix}$$

of order 2 in Subsection IV-A.

**Definition 14:** A generalized delay matrix $D(z)$ with multi-variables $z = (z_0, z_1, \cdots, z_{n-1})$ is the Kronecker product of $D(z_v)$ for $0 \leq v < n$, i.e.,

$$D(z) = D(z_{n-1}) \otimes \cdots \otimes D(z_1) \otimes D(z_0). \quad (43)$$

It is obvious that $D(z)$ is also a diagonal matrix, so we can write $D(z)$ by

$$D(z) = diag(\phi_0(z), \phi_1(z), \cdots, \phi_{N-1}(z)),$$

where $\phi_y(z)$ ($0 \leq y < N$) is a function of $z$.

**Example 12:** Let $N = 2^2$ and $z = (z_0, z_1)$. The generalized delay matrix $D(z_0, z_1)$ can be written in the form of

$$D(z_0, z_1) = \begin{bmatrix} 1 & 0 \\ 0 & z_{1} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & z_{0} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & z_0 & 0 & 0 \\ 0 & 0 & z_1 & 0 \\ 0 & 0 & 0 & z_1 z_0 \end{bmatrix} = \begin{bmatrix} z_1^0 \cdot z_0^0 & 0 & 0 & 0 \\ 0 & z_0^0 \cdot z_1^0 & 0 & 0 \\ 0 & 0 & z_1^1 \cdot z_0^0 & 0 \\ 0 & 0 & 0 & z_1^1 \cdot z_0^1 \end{bmatrix}.$$  

From the above example, $\phi_y(z)$ in the main diagonal can be expressed by $z_1^{x_1} \cdot z_0^{x_0}$, where $(x_0, x_1)$ is the binary expansion of integer $y$. In general, the generalized delay matrix $D(z)$ can be explicitly represented by the following lemma.

**Lemma 8:** Let $(x_0, x_1, \cdots, x_{n-1})$ be the binary expansion of integer $y$, i.e., $y = \sum_{i=0}^{n-1} x_i \cdot 2^i$. Then the generalized delay matrix $D(z)$ in Definition 14 can be expressed as

$$D(z) = \begin{bmatrix} \phi_0(z) & 0 & \cdots & 0 \\ 0 & \phi_1(z) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \phi_{N-1}(z) \end{bmatrix},$$

where

$$\phi_y(z) = \prod_{i=0}^{n-1} z_{v_i}^{x_i}. \quad (44)$$

We omit the proof of the above lemma, since it can be easily done by mathematical induction.

Let $H^{(k)}$ be an arbitrary BH matrix chosen from $H(q, N)$ for $0 \leq k \leq m$ and $D(z_k)$ be the generalized delay matrix from Definition 14 where $z_k = (z_{kn}, z_{kn+1}, \cdots, z_{kn+n-1})$ for $0 \leq k < m$. And let $z = (z_0, z_1, \cdots, z_{m-1}) = (z_0, z_1, \cdots, z_{n-1})$. We define a multivariate polynomial matrix $M(z)$ as follows.

$$M(z) = H^{(0)} \cdot D(z_0) \cdot H^{(1)} \cdot D(z_1) \cdot \cdots \cdot H^{(m-1)} \cdot D(z_{m-1}) \cdot H^{(m)} \cdot \left( \prod_{k=0}^{m-1} (H^{(k)} \cdot D(z_k)) \right) \cdot H^{(m)} \quad (45)$$

**Remark 8:** The matrix $M(z)$ defined here is similar to the seed PU matrix defined in Subsection IV-A, but the delay matrices are chosen differently. Let $\pi$ be a permutation of $\{0, 1, \cdots, mn-1\}$ and $z_0 = Z^{\pi(0)}$ in $M(z)$ for $0 \leq t < mn$, we obtain a matrix $M(Z)$, which is identical to the univariable PU matrix proposed in [26].

**Theorem 6:** $M(z)$ defined in formula (45) is a desired PU matrix, i.e.,

1. $M(z) \cdot M^T(z) = 2^{(m+1)n} \cdot I_N$;
2. Each entry of $M(z)$ can be expressed by the generating function of a GBF $f(x) : \mathbb{Z}_2^{mn} \rightarrow \mathbb{Z}_q$ for $x = (x_0, x_1, \cdots, x_{mn-1})$.

**Proof:** It is obvious that $M(z) \cdot M^T(z) = 2^{(m+1)n} \cdot I_N$.

We expand $M(z)$ in the following form.

$$M(z) = \sum_{x \in \mathbb{Z}_2^{mn}} (M(x) \cdot z^x),$$

where matrix $M(x)$ is the coefficient matrix of matrix $M(z)$ of term $z^x = z_{0}^{x_0} \cdot z_{1}^{x_1} \cdots z_{mn-1}^{x_{mn-1}}$.

Based on formula (44), the generalized delay matrix $D(z_k)$ can be represented by

$$D(z_k) = \sum_{y_k \in \mathbb{Z}_2^n} (E_{y_k} \cdot \phi_{y_k}(z_k)),$$

where $y_k = \sum_{v=0}^{n-1} x_{kn+v} \cdot 2^v$ and $E_i$ is a matrix with single-entry 1 at $(i, i)$ and zero elsewhere.
On the other hand,
\[
M(z) = \left( \prod_{k=0}^{m-1} \left( H^{(k)} \cdot D(z_k) \right) \right) \cdot H^{(m)}
= \left( \prod_{k=0}^{m-1} \left( H^{(k)} \cdot \sum_{y_k \in \mathbb{Z}_{2^n}} (E_{y_k} \cdot \phi_{y_k}(z_k)) \right) \right) \cdot H^{(m)}
= \sum_{y_0 \in \mathbb{Z}_{2^n}} \cdots \sum_{y_{m-1} \in \mathbb{Z}_{2^n}} \left( \prod_{k=0}^{m-1} \left( H^{(k)} \cdot E_{y_k} \right) \cdot H^{(m)} \right) \prod_{k=0}^{m-1} \phi_{y_k}(z_k)
= \sum_{x \in \mathbb{Z}_{2^m}} \left( \prod_{k=0}^{m-1} \left( H^{(k)} \cdot E_{y_k} \right) \cdot H^{(m)} \right) .^x .
\]

Thus we have
\[
M(x) = \left( \prod_{k=0}^{m-1} \left( H^{(k)} \cdot E_{y_k} \right) \right) .^H .^{(m)},
\]

and each entry
\[
M_{i,j}(x) = H^{(0)}_{i,j_0} \cdot \left( \prod_{k=1}^{m-1} H^{(k)}_{y_k-1,y_k} \right) .^H .^{(m)}_{y_{m-1},j}.
\]

Therefore, for given i and j, there exist GBF \( f_{i,j} \) from \( \mathbb{Z}_{2^m} \) to \( \mathbb{Z}_q \) such that \( M_{i,j}(z) \) equals
\[
\sum_{x_0=0}^{1} \cdots \sum_{x_{m-1}=0}^{1} (\omega_{f_{i,j}}(x_0,x_1,\cdots,x_{m-1}) .^x \cdot z^x)
\]
which complete the proof.

\( M(z) \) in formula (45) is called a generalized seed PU matrix. Let both the order of the seed PU matrices in Subsection IV-A and the generalized seed PU matrices be \( N = 2^n \). Then we have
\[
\omega_{f_{i,j}}(y_0,y_1,\cdots,y_{m-1}) = H^{(0)}_{i,j_0} \cdot \left( \prod_{k=1}^{m-1} H^{(k)}_{y_k-1,y_k} \right) .^H .^{(m)}_{y_{m-1},j},
\]
from formula (22), and
\[
\omega_{f_{i,j}}(x_0,x_1,\cdots,x_{m-1}) = H^{(0)}_{i,j_0} \cdot \left( \prod_{k=1}^{m-1} H^{(k)}_{y_k-1,y_k} \right) .^H .^{(m)}_{y_{m-1},j},
\]
from formula (46), respectively, where \( y_k = \sum_{v=0}^{n-1} x_{kn+v} \cdot 2^v \).

Consequently we have
\[
f_{i,j}(x_0,x_1,\cdots,x_{m-1}) = f_{i,j}(y_0,y_1,\cdots,y_{m-1}).
\]

Therefore, if we replace \( y = (y_0,y_1,\cdots,y_{m-1}) \) by \( x = (x_0,x_1,\cdots,x_{m-1}) \), then the GBFs extracted from the generalized seed PU matrices are identical to the functions extracted from the seed PU matrices. However, functions \( f_{i,j}(y) \) extracted from the seed PU matrices are the arrays of size \( 2^n \times 2^n \times \cdots \times 2^n \) and dimension \( m \), while the GBFs \( f_{i,j}(x) \) extracted from the generalized seed PU matrices are arrays of size \( 2 \times 2 \times \cdots \times 2 \) and dimension \( mn \).

\section*{B. Constructions From the Generalized Seed PU Matrices}

We now extend the results in Theorem 5 for \( N = 2^n \). Recall \( y_k = \sum_{v=0}^{n-1} x_{kn+v} \cdot 2^v \), \( y = (y_0,y_1,\cdots,y_{m-1}) \), and \( x = (x_0,x_1,\cdots,x_{m-1}) \).

\textbf{Theorem 7:} For \( N = 2^n \), suppose that \{\( f_{i,j}(y) \)\} and \{\( f_{i,j}(y) \)\} respectively form a CAS and a CCC of size \( N \) \((0 \leq i,j < N)\), where both \( f_{i,j} \) and \( f_{i,j} \) are given in Theorem 5. By replacing the functions \( f_{i,j}(y) \) and \( f_{i,j}(y) \) by GBFs \( f_{i,j}(x) \) and \( f_{i,j}(x) \) respectively, for arbitrary permutation \( \pi \) of symbols \{0, 1, \cdots, \( mn - 1 \} \), we have

1. The sequences evaluated by the following GBFs form a CAS of size \( N \):
\[
\pi \cdot f_{i,j}(x) = f_{i,j}(x_{\pi(0)},x_{\pi(1)},\cdots,x_{\pi(mn-1)}).
\]

2. The sequences evaluated by the following GBFs form a CCC of size \( N \) and length \( N^m \):
\[
\pi \cdot f_{i,j}(x) = f_{i,j}(x_{\pi(0)},x_{\pi(1)},\cdots,x_{\pi(mn-1)}).
\]

From Theorem 7, the results in Constructions 3 and 4 in Section V can be extended to the following Constructions 5 and 6 respectively.

\textbf{Construction 5:} Let \( \pi \) be a permutation of \{0, 1, \cdots, \( 2m-1 \} \) and \( x = (x_0,x_1,\cdots,x_{2m-1}) \). For \( N = 4 \) and \( q = 2 \), the GBFs extracted from the generalized seed PU matrices are the same as (41).

1. The corresponding function matrix \( \tilde{M}(x) \) is given by
\[
\tilde{M}(x) = f \cdot J_4 + A(x_0,x_1) \cdot J_4 + J_4 \cdot A(x_{2m-2},x_{2m-1}),
\]
where the GBF \( f \) is in the form (41) and \( A(x_0,x_1) = diag\{0,x_0,x_1 + x_1\} \) is a diagonal matrix. The sequences evaluated by the matrix \( \pi \cdot \tilde{M}(x) \) form a CCC of size \( 4 \).

2. The collection of binary sequences in CSSs of size 4 derived from the generalized seed PU matrices can be expressed by
\[
S'((2,4)) = \left\{ \sum_{k=1}^{m-1} h_k(x_{\pi(2-k)},x_{\pi(2-1)},x_{\pi(2)},x_{\pi(2+k-1)}) \right\} + \sum_{k=0}^{m-1} \left\{ d_k x_{\pi(2k-1)} + c_k x_{\pi(k)} + c' \right\}
\]
for \( h_k(\cdots,\cdots) \in \delta_{\mathbb{Q}}(2,4) \{1 \leq k \leq m-1 \} \) and \( d_k,c_k,c' \in \mathbb{Z}_2 \), \( 0 \leq k \leq m-1 \).

3. The sequences evaluated by
\[
\left\{ \begin{array}{l}
f, \\
f + x_{\pi(0)}, \\
f + x_{\pi(1)}, \\
f + x_{\pi(0)} + x_{\pi(1)}
\end{array} \right.
\]
form a binary CSS of size 4 for \( \forall f \in S'((2,4)) \).

\textbf{Construction 6:} Let \( \pi \) be a permutation of \{0, 1, \cdots, 2m-1 \} and \( x = (x_0,x_1,\cdots,x_{2m-1}) \). For \( N = 4 \) and \( q = 4 \), the GBFs extracted from the generalized seed PU matrices are the same as (42).
(1) The corresponding function matrix \(\widetilde{M}(x)\) is given by
\[
\widetilde{M}(x) = f \cdot J_4 + A(x_0, x_1) \cdot J_4 + J_4 \cdot B(x_{2m-2}, x_{2m-1}),
\]
where the GBF \(f\) is in the form (42) and the diagonal matrices \(A(x_0, x_1), B(x_0, x_1)\) are arbitrarily chosen from the set \(\{\text{diag}(0, 2x_0, 2x_1, 2x_0 + 2x_1), \text{diag}(0, 2x_0 + x_1, 2x_0, 3x_1), \text{diag}(0, x_0 + 3x_1 + 2x_0x_1, 2x_0 + 2x_1, 3x_0 + x_1 + 2x_0x_1)\}\). The sequences evaluated by the matrix \(\pi \cdot \widetilde{M}(x)\) form a CCC of size 4.

(2) The collection of quaternary sequences in CSSs of size 4 derived from the generalized seed PU matrices can be represented by
\[
S'(4, 4) = \left\{ \sum_{k=1}^{m-1} h_k(x_{\pi(2k-2)}, x_{\pi(2k-1)}, x_{\pi(2k)}, x_{\pi(2k+1)}) + \sum_{k=0}^{2m-1} d_k x_{\pi(2k+1)} + c_k x_k + c' \right\}
\]
for \(h_k(\cdot, \cdot, \cdot) \in \delta_Q(4, 4)\) \((1 \leq k \leq m - 1)\) and \(d_k, c_k, c' \in \mathbb{Z}_4, 0 \leq k \leq m - 1\).

(3) The sequences evaluated by
\[
f, \quad f + 2x_{\pi(0)}, \quad f + 2x_{\pi(1)}, \quad f + 2x_{\pi(0)} + 2x_{\pi(1)},
\]
form a complementary set of size 4 for \(\forall f \in S'(4, 4)\).

The sequences obtained by Theorem 7 are the union of the orbits of the functions extracted from the seed PU matrix of order \(2^n\) under the action of all permutations of Boolean variable \(x\), whereas the sequences obtained by Theorem 5 are the union of orbits of these functions under the action of all permutations of variable \(y\), which can be regarded as a subgroup of the permutations of Boolean variable \(x\). There are \((mn)!\) permutations can be applied in Theorem 7, whereas only \(m!\) permutations can be applied in Theorem 5. We give an example for \(N = q = 4\) and \(m = 3\) in Construction 6 to show that new sequences are produced by Theorem 7. Let \(f(x) = f(y) = h_1(y_0, y_1) + h_2(y_1, y_2)\), where \(h_1\) and \(h_2\) are respectively with the form \(\psi_5\) and \(\psi_8\) in \(\delta_Q(4, 4)\).

Then the cubic terms of \(\pi \cdot f(x) = 2x_0x_2x_4 + 2x_1x_3x_5\) for \(\pi(0, 1, 2, 3, 4, 5, 6) = (0, 2, 4, 1, 3, 5)\). Note that the indices of the terms \(2x_0x_2x_4\) (or \(2x_1x_3x_5\)) are all even (or all odd) and these functions \(\pi \cdot f(x)\) cannot be produced in Construction 4.

Remark 9: From the constructions above, the set \(S_{L}(q, N = 2^n)\) is no longer an invariant under the permutations of the Boolean variables \(x\), so the enumeration method in Subsection IV-E cannot be applied here. The enumeration of the sequences constructed in Theorem 7 is a difficult problem, which will be a future work.

VII. RECURSIVE CONSTRUCTIONS OF DESIRED PU MATRICES AND CORRESPONDING CSSS AND CCCS

The motivation of this section is to find some recursive constructions of the desired PU matrices and their corresponding GBF matrices. We first propose two recursive constructions by the seed PU matrices of order 2, from which not only the GBF-based constructions of CSSs [33], [42] and CCCs [38] are explained from the viewpoint of PU matrices, but also new GBF-based constructions of CCCs are produced. Then we generalize these two recursive constructions by the desired PU matrices of higher order. And new GBF-based constructions of CSSs and CCCs are produced correspondingly.

We first introduce the notations and give a lemma, which will be applied to determine the corresponding GBF matrix from its generating matrix. Define variables
\[
\begin{align*}
\begin{cases}
  z_0 = (z_0, z_1, \ldots, z_{n-1}), \\
  z_1 = (z_n, z_{n+1}, \ldots, z_{n+m-1}), \\
  z_2 = (z_{n+m_1}, z_{n+m_1+1}, \ldots, z_{n+m_1+m-1}), \\
  (z_0, z_1, z_2) = (z_0, z_1, \ldots, z_{n+m_1+m-1})
\end{cases}
\end{align*}
\]
and corresponding Boolean variables
\[
\begin{align*}
\begin{cases}
  x_0 = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{Z}_2^n, \\
  x_1 = (x_n, x_{n+1}, \ldots, x_{n+m-1}) \in \mathbb{Z}_2^m, \\
  (x_0, x_1) \in \mathbb{Z}_2^{m_1}, \\
  (x_0, x_1, x_2) = (x_0, x_1, \ldots, x_{n+m_1+m-2}) \in \mathbb{Z}_2^{m_1+m_2}
\end{cases}
\end{align*}
\]
Let \(A(z_1)\) and \(B(z_2)\) be the generating matrices of the GBF matrices \(A(x_1) = \{a_i, j(x_1)\}\) and \(B(x_2) = \{b_i, j(x_2)\}\) of size \(N = 2^n\) respectively, where \(a_i, j(x_1)\) and \(b_i, j(x_2)\) are GBFs from \(\mathbb{Z}_q^{m_1}\) to \(\mathbb{Z}_q\) and \(\mathbb{Z}_q^{m_2}\) to \(\mathbb{Z}_q\) respectively. Note that \(A(z_1)\) and \(B(z_2)\) are not required to be PU matrices here.

Recall the generalized delay matrix \(D(z_0)\) of order \(N = 2^n\) in Definition 14 and the basis function \(\delta_i : \mathbb{Z}_N \rightarrow \mathbb{Z}_q\) shown in Example 10.

Lemma 9: Let \(C(z_0, z_1, z_2)\) be a multivariate polynomial matrix defined by
\[
C(z_0, z_1, z_2) = A(z_1) \cdot D(z_0) \cdot B(z_2).
\]

Then \(C(z_0, z_1, z_2)\) is the generating matrix of the GBF matrix \(C(x_0, x_1, x_2)\), where each entry is a GBF from \(\mathbb{Z}_2^{m_1+m_2}\) to \(\mathbb{Z}_q\) with the expression
\[
c_{r,s}(x_0, x_1, x_2) = \sum_{i=0}^{N-1} (d_{r,i}(x_1) + b_{i, s}(x_2)) \delta_i(x_0)
\]
for \(0 \leq r, s < N\). Moreover, if both \(A(z_1)\) and \(B(z_2)\) are desired PU matrices, then \(C(z_0, z_1, z_2)\) is also a desired PU matrix.

Proof: See Appendix A.
Example 13: Here comes a simple example for \( N = q = 2 \), assume that \( A(\pi_{01}) = \begin{bmatrix} 1 + z_{1} & 1 - z_{2} \\ 1 - z_{1} & 1 + z_{2} \end{bmatrix} \) and \( B(\pi_{0}) = \begin{bmatrix} 1 + x_{1} \\ 1 \end{bmatrix} \). Then their GBF matrices are \( \tilde{A}(\pi_{01}) = \begin{bmatrix} 1 - x_{0} \\ x_{0} \end{bmatrix} \) and \( \tilde{B}(\pi_{0}) = \begin{bmatrix} 0 \\ x_{2} \end{bmatrix} \) respectively. Let \( C(z_{0}, z_{1}, z_{2}) = A(\pi_{01}) \cdot D(z_{0}) \cdot B(\pi_{0}) \). From Lemma 9, we obtain the GBF matrix
\[
\tilde{C}(x_{0}, x_{1}, x_{2}) = \begin{bmatrix} 1 - x_{0} \\ x_{0} \end{bmatrix} \begin{bmatrix} 1 - x_{0} \\ x_{0} \end{bmatrix} + \begin{bmatrix} 1 - x_{0} \\ x_{0} \end{bmatrix} \begin{bmatrix} 0 \\ x_{2} \end{bmatrix} = (x_{0}x_{1} + x_{0}x_{2} + x_{0}) \cdot J_{2} + \begin{bmatrix} 0 \\ x_{2} \end{bmatrix}.
\]

A. Recursive Constructions of CSSs and CCCs From GAPs

In this subsection, we propose new construction of desired PU matrices by the seed PU matrices of order 2. We will show in next subsection that the GBF-based constructions of CSSs proposed in [33], [42] and CCCs proposed in [38] are all special cases of the CSSs and CCCs derived from the new desired PU matrices, introduced below.

We denote the seed PU matrix of order 2 by \( U(z) \). Its corresponding GBF matrix, denoted by \( \tilde{U}(x) \), is well studied in Subsection V-A. We have
\[
\tilde{U}(x) = f(x) \cdot J_{2} + q \begin{bmatrix} 0 \\ x_{\pi_{0}} - x_{\pi_{0} + x_{\pi_{0} - 1}} \end{bmatrix},
\]
where
\[
f(x) = q \sum_{k=1}^{m-1} x_{\pi_{k} - 1} x_{\pi_{k}} + \sum_{k=0}^{m-1} c_{k} x_{k} + c'.
\]

Definition 15: Let \( P \) be a permutation matrix of order \( 2^{n+1} \) with entries
\[
P_{u, v} = \begin{cases} 1, & \text{if } v \equiv 2u \mod 2^{n+1} - 1 \\ 0, & \text{otherwise} \end{cases}
\]
for \( 0 \leq u, v < 2^{n+1} \). In other word, \( P_{u, v} = 1 \) if and only if \((u, v, u_{0}, u_{1}, \ldots, u_{n-1}) = (v_{0}, v_{1}, v_{2}, v_{3}, v_{4}, v_{5}, v_{6}, v_{7}, v_{8}, v_{9}, v_{10}, v_{11}, v_{12}, v_{13}, v_{14}, v_{15})\) where \((u_{0}, u_{1}, \ldots, u_{n})\) and \((v_{0}, v_{1}, \ldots, v_{n})\) are the binary expansions of integers \( u \) and \( v \) respectively.

For \( 0 \leq j < 2^{n} \), let \( U^{(j)}(z) \) be the generating matrix of the GBF matrix \( \tilde{U}^{(j)}(x) \) with the form (49), where the function \( f(x) \) and permutation \( \pi \) are replaced by \( f^{(j)}(x) \) and \( \pi_{j} \), respectively. Suppose that \( \tilde{H}^{(0)}, \tilde{H}^{(1)} \in H(q, 2^{n}) \) and their corresponding phase matrices are \( \tilde{H}^{(0)}, \tilde{H}^{(1)} \).

Theorem 8: Let matrices \( P, H^{(0)}, H^{(1)} \) and \( U^{(j)}(z) \) be given as above. Define a multivariate polynomial matrix of order \( 2^{n+1} \) by
\[
G(z) = \begin{bmatrix} H^{(0)} \\ 0 \\ H^{(1)} \end{bmatrix} \cdot P.
\]

If we set
\[
H^{(0)} = H^{(1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ \end{bmatrix},
\]

Then \( G(z) \) is a desired PU matrix and the entries of its corresponding GBF \( \tilde{G}(x) \) are functions from \( \mathbb{Z}_{2}^{m} \) to \( \mathbb{Z}_{q} \) with the expression
\[
\tilde{G}_{u, v}(x) = f^{(j)}(x) + \frac{q}{2} \alpha x_{\pi_{j}(0)} + \frac{q}{2} \beta x_{\pi_{j}(m-1)} + \tilde{H}_{\pi_{j}}(x),
\]
where \( u = \alpha \cdot 2^{n} + i \) and \( v = \beta \cdot 2^{n} + j \) \((0 \leq \alpha, \beta \leq 1, 0 \leq i, j < 2^{n}) \).

Proof: See Appendix B.

Theorem 8 provides a GBF-based construction of CCCs, in which the sequences are Golay sequences proposed by Davis and Jedwab in [10]. We give an example of \( G(z) \) of order 8 and its corresponding GBF matrix in the following example.

Example 14: For convenience, the PU matrices \( U^{(j)}(z) \) of order 2 are denoted by \( \begin{bmatrix} A_{j} & B_{j} \\ C_{j} & D_{j} \end{bmatrix} \) and their corresponding GBF matrices \( \tilde{U}^{(j)}(x) \) are denoted by \( \begin{bmatrix} a_{j} & b_{j} \\ c_{j} & d_{j} \end{bmatrix} \) for \( 0 \leq j < 4 \).

Let \( P \) be a permutation matrix of order 8 in Definition 15. Then the entry \( P_{u, v} = 1 \) iff \((u, v)\) belongs to \( \{(0, 0), (1, 2), (2, 4), (3, 6), (4, 1), (5, 3), (6, 5), (7, 7)\} \), i.e.,
\[
P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.
\]

Then we have
\[
P \cdot \begin{bmatrix} A_{0} & B_{0} \\ C_{0} & D_{0} \end{bmatrix} = \begin{bmatrix} A_{1} & B_{1} \\ C_{1} & D_{1} \end{bmatrix},
\]
\[
P \cdot \begin{bmatrix} A_{2} & B_{2} \\ C_{2} & D_{2} \end{bmatrix} = \begin{bmatrix} A_{3} & B_{3} \\ C_{3} & D_{3} \end{bmatrix}.
\]
then we have
\[
G(z) = \begin{bmatrix}
A_0 & A_1 & A_2 & A_3 & B_0 & B_1 & B_2 & B_3 \\
A_0 - A_1 & A_2 - A_3 & B_0 - B_1 & B_2 - B_3 \\
A_0 & A_1 - A_2 & A_3 - B_0 & B_1 - B_2 \\
A_0 - A_1 & A_2 - A_3 & B_0 - B_1 & B_2 - B_3 \\
C_0 - C_1 & C_2 - C_3 & D_0 - D_1 & D_2 - D_3 \\
C_0 & C_1 - C_2 & C_3 - D_0 & D_1 - D_2 - D_3 \\
C_0 & C_1 & C_2 - D_0 & D_1 - D_2 - D_3 \\
C_0 & -C_1 & -C_2 & D_0 - D_1 - D_2 - D_3
\end{bmatrix},
\]
and its corresponding function matrix can be expressed by
\[
\tilde{G}(x) = \begin{bmatrix}
a_0 & a_1 & a_2 & a_3 & b_0 & b_1 & b_2 & b_3 \\
a_0 + a_1 & a_2 + a_3 & b_0 + b_1 & b_2 + b_3 \\
a_0 + a_1 & a_2 + a_3 & b_0 + b_1 & b_2 + b_3 \\
a_0 + a_1 & a_2 + a_3 & b_0 + b_1 & b_2 + b_3 \\
a_0 + a_1 & a_2 + a_3 & b_0 + b_1 & b_2 + b_3 \\
a_0 + a_1 & a_2 + a_3 & b_0 + b_1 & b_2 + b_3 \\
a_0 + a_1 & a_2 + a_3 & b_0 + b_1 & b_2 + b_3 \\
a_0 + a_1 & a_2 + a_3 & b_0 + b_1 & b_2 + b_3
\end{bmatrix}.
\]
Before introducing another type of desired PU matrices, we define variables
\[
\begin{align*}
z_0 &= (z_0, z_1, \ldots, z_{m-1}), \\
z_1 &= (z_m, z_{m+1}, \ldots, z_{m+n-1}),
\end{align*}
\]
and corresponding Boolean variables
\[
\begin{align*}
x_0 &= (x_0, x_1, \ldots, x_{m-1}) \in \mathbb{Z}_2^m, \\
x_1 &= (x_m, x_{m+1}, \ldots, x_{m+n-1}) \in \mathbb{Z}_2^n.
\end{align*}
\]
Let \( G(z_0) \) be a desired PU matrix of order \( 2^n+1 \) obtained from Theorem 8, and \( G(x_0) \) its corresponding GBF matrix.

Theorem 9: Let matrices \( G(z_0), H^{(2)} \) and \( H^{(3)} \) be given as above. Then \( M(z_0, z_1) \) defined by
\[
M(z_0, z_1) = G(z_0) \begin{bmatrix} D(z_1) & 0 \\ 0 & D(z_1) \end{bmatrix} \begin{bmatrix} H^{(2)} & 0 \\ 0 & H^{(3)} \end{bmatrix}
\]
is a desired PU matrix, and the entries of its corresponding GBF \( \tilde{M}(x_0, x_1) \) are the functions from \( \mathbb{Z}_2^{m+n} \) to \( \mathbb{Z}_2 \) with the expression
\[
\tilde{M}_{u,v}(x_0, x_1) = \sum_{i=0}^{2^n-1} \left( f^{(i)}(x_0) + q \alpha x_{\pi_i(0)} \right) + q \frac{\beta}{2} x_{\pi_i(m-1)} \delta_i(x_1),
\]
where \( u = \alpha \cdot 2^n + l \) and \( v = \beta \cdot 2^n + j \) for \( 0 \leq \alpha, \beta \leq 1 \) and \( 0 \leq l, j < 2^n \).

Proof: See Appendix C.

B. Instantiations of the Recursive Constructions

In this subsection, we will show that the known GBF-based constructions of CSSs and CCCs in the literature are our instantiations of special cases of Theorems 9. Let \( H^{(k)} \) \( (0 \leq k \leq 3) \) in Theorems 8 and 9 be WHT matrices, i.e., \( H^{(k)}_{i,j} = (-1)^{i+j} \), where \( i \) and \( j \) are the binary expansions of integer \( i \) and \( j \) respectively, and \( i \cdot j \) denotes the dot product over \( \mathbb{Z}_2 \). By studying \( M_{0,0}(x_0, x_1) \) in formula (57), we have the following corollary.

Corollary 4: The array (GBF)
\[
f(x_0, x_1) = \sum_{i=0}^{2^n-1} f^{(i)}(x_0) \delta_i(x_1)
\]
from \( \mathbb{Z}_2^{m+n} \) to \( \mathbb{Z}_2 \) lies in a CAS of size \( 2^n+1 \).

From Corollary 4, we have \( f(x_0, x_1)_{|x_1=i} = f^{(i)}(x_0) \). Therefore, the sequences proposed in [42] are evaluated by the GBF: \( \pi \cdot f(x_0, x_1) \), where \( f(x_0, x_1) \) is shown in formula (58) and \( \pi \) is an arbitrary permutation of binary variables \( (x_0, x_1) \).

The sequences proposed in [33] are a subset of those sequences when the permutation \( \pi \) in functions \( f^{(i)}(x_0) \) are the identity permutation for all \( i \) and \( f(x_0, x_1) \) is a quadratic GBF.

Moreover, the GBFs of CCA constructed in Theorem 9 can be expressed in the following form.

Corollary 5: Let \( f(x_0, x_1) \) be of the form (58). For \( 0 \leq u, v \leq 2^n+1 \), the arrays (GBFs)
\[
f_{u,v}(x_0, x_1) = f(x_0, x_1) + q \frac{\alpha}{2} (i \cdot x_1 + j \cdot x_1)
\]
\[
+ q \beta \frac{\alpha}{2} \sum_{i=0}^{2^n-1} x_{\pi_i(0)} \delta_i(x_1) + q \beta \frac{\alpha}{2} \sum_{i=0}^{2^n-1} x_{\pi_i(m-1)} \delta_i(x_1)
\]
form a CCA of size \( 2^n+1 \), where \( u = \alpha \cdot 2^n + i \) and \( v = \beta \cdot 2^n + j \) for \( 0 \leq \alpha, \beta \leq 1 \) and \( 0 \leq i, j < 2^n \).

For some special cases, the GBFs in Corollary 5 can be represented by the sum of \( f(x_0, x_1) \) and a linear term.

Corollary 6: With the same notations as Corollary 5, let \( f(x_0, x_1) \) be of the form (58) and every \( \pi_i \) in \( f^{(i)}(x_0) \) be the identity permutation for \( 0 \leq i \leq 2^n-1 \). For \( 0 \leq u, v \leq 2^n+1 \), the arrays (GBFs)
\[
f_{u,v}(x_0, x_1)
\]
\[
= f(x_0, x_1) + q \frac{\alpha}{2} (i \cdot x_1 + j \cdot x_1 + \alpha x_0 + \beta x_{m-1})
\]
form a CCA of size \( 2^n+1 \).

The CCCs proposed in [38] based on the CSSs constructed in [33] is a special case of Corollary 6 by applying action of permutations on binary variables \( (x_0, x_1) \) when \( f(x_0, x_1) \) is a quadratic function. Furthermore, Corollary 5 shows new GBF-based construction of CCCs based on the CSSs constructed in [42].

Remark 10: From Corollaries 4 and 6, GBF-based construction of CSSs in [33], [42] and CCCs in [38] are all derived from CASs and CCAs of size \( 2 \times 2 \times \cdots \times 2 \).

C. Generalized Recursive Constructions

From Theorem 9, we have shown that CSSs in [33], [42] and CCCs in [38] can be derived from the seed PU matrices of order 2 (or WHT matrices). Section V shows that CSSs and CCCs extracted from the seed PU matrices involving other BH matrices have not been considered in the literature. In this section, we generalize the results in Theorems 8
and 9 by applying desired PU matrices with flexible orders. Consequently, new CSSs and CCCs can be constructed from Theorem 1.

The first generalization is immediately from Theorem 8. Let \(U^{(j)}(z_0)\) \((0 \leq j < 2^n)\) and \(V^{(\alpha)}(z_1)\) \((0 \leq \alpha < 2^n)\) be desired PU matrices of order \(2^n\) and \(2^n\), whose corresponding GBF matrices are \(\tilde{U}^{(j)}(x_0)\) and \(\tilde{V}^{(\alpha)}(x_1)\), respectively, where

\[
\begin{align*}
&z_0 = (z_0, z_1, \ldots, z_{m-1}), \\
&z_1 = (z_m, z_{m+1}, \ldots, z_{m+m'-1}), \\
&x_0 = (x_0, x_1, \ldots, x_{m-1}) \in \mathbb{Z}_2^m, \\
&x_1 = (x_m, x_{m+1}, \ldots, x_{m+m'-1}) \in \mathbb{Z}_2^{m'}.
\end{align*}
\]

and Boolean variables

\[
\begin{align*}
&\left\{ x_0 = (x_0, x_1, \ldots, x_{m-1}) \in \mathbb{Z}_2^m, \\
&x_1 = (x_m, x_{m+1}, \ldots, x_{m+m'-1}) \in \mathbb{Z}_2^{m'} \right. \\
&\left. \text{where } u, v < 2^n \right. \\
&\left. \text{and } \alpha, \beta \leq 2^n \right. \\
&\left. \text{and } \{g_{\alpha, \beta}\} \right. \\
&\left. \text{is an array of size } 2^n \times 2^n \right. \\
&\left. \text{lying in a CAS of size } 2^n \times 2^n \right. \\
&\left. \text{and } P \text{ is a permutation matrix of order } 2^n \right. \\
&\left. \text{and } P' \text{ is a permutation matrix of order } 2^n \right. \\
&\left. \text{such that } PU^{(j)}(z_0) = P' U^{(j)}(z_0) \right. \\
&\left. \text{and } PU^{(\alpha)}(z_1) = P' U^{(\alpha)}(z_1) \right. \\
&\left. \text{for } 0 \leq j < 2^n \text{ and } 0 \leq \alpha < 2^n \right.
\end{align*}
\]

Then we have the following results.

**Theorem 10:** Let \(P\) be a permutation matrix of order \(2^{n+m'}\) with each entry \(P_{u,v} = 1\) if and only if \(v = 2^n u + i\) (mod \(2^{n+m'} - 1\)). Let \(\tilde{U}^{(j)}(z_0)\) \((0 \leq j < 2^n)\) and \(\tilde{V}^{(\alpha)}(z_1)\) \((0 \leq \alpha < 2^n)\) shown above. Define a multivariate polynomial matrix of order \(2^{n+m'}\) by \(G(z_0, z_1)\) which is given in (63), shown at the bottom of the page.

Then \(G(z_0, z_1)\) is a desired PU matrix of order \(2^{n+m'}\). And it is the generating matrix of GBF matrix \(G(x_0, x_1)\) whose entries are GBFs from \(\mathbb{Z}_2^{2^{n+m'}}\) to \(\mathbb{Z}_2\) with the expression

\[
\tilde{G}_{u,v}(x_0, x_1) = \tilde{U}^{(j)}(x_0) + \tilde{V}^{(\alpha)}(x_1),
\]

where \(u = \alpha \cdot 2^n + i\) and \(v = \beta \cdot 2^n + j\) for \(0 \leq \alpha, \beta \leq 2^n\) and \(0 \leq i, j < 2^n\).

We omit the proof of Theorem 10 since it is similar to the proof of Theorem 8. Formula (64) shows new GBF-based constructions of CCCs and CSSs. Moreover, Theorem 10 can be used to provide a better PMEPR bound.

**Corollary 7:** Let \(f_0(x_0)\) and \(f_1(x_1)\) be two arrays (GBFs) lying in CASs of size \(2^n\) and \(2^n\), respectively. Then the GBF

\[
f(x_0, x_1) = f_0(x_0) + f_1(x_1)
\]

is an array of size \(2^n \times 2^n\) lying in a CAS of size \(2^{n+m'}\). The sequence evaluated by GBF \(\pi \cdot f(x_0, x_1) + f'(x_0, x_1)\) lies in a CSS of size \(2^{n+m'}\), where \(\pi\) is a permutation of Boolean variables \((x_0, x_1)\) and \(f'(x_0, x_1)\) is an affine GBF.

**Remark 11:** If \(U^{(j)}(z_0) = U(z_0)\) for \(0 \leq j < 2^n\) and \(V^{(\alpha)}(z_1) = V(z_1)\) for \(0 \leq \alpha < 2^n\) in Theorem 10, then we have

\[
G(z_0, z_1) = U(z_0) \otimes V(z_1).
\]

Next we generalize the results in Theorem 9. Let \(V(z_1)\) and \(U^{(\beta)}(z_2)\) \((0 \leq \beta < 2^n)\) be desired PU matrices of order \(2^{n+m'}\) and \(2^n\), whose corresponding GBF matrices are \(\tilde{V}(x_1)\) and \(\tilde{U}^{(\beta)}(x_2)\), respectively. Note that here \(z_0, z_1, z_2\) and \(x_0, x_1, x_2\) are defined the same as those in (47) and (48), respectively. Then we have the following theorem.

**Theorem 11:** Let matrices \(V(z_1)\) and \(U^{(\beta)}(z_2)\) \((0 \leq \beta < 2^n)\) be given as above. Then \(M(z_0, z_1, z_2)\) given in (65), shown at the bottom of the page, is a desired PU matrix.

And it is the generating matrix of GBF matrix \(M(x_0, x_1, x_2)\) whose entries are functions from \(\mathbb{Z}_2^{2^{n+m'+2^n}}\) to \(\mathbb{Z}_2\) with the expression

\[
\tilde{M}_{u,v}(x_0, x_1, x_2) = \sum_{i=0}^{2^n-1} \left( \tilde{V}_{i,u} \cdot 2^{n+i}(x_1) + \tilde{U}^{(\beta)}_{i,v}(x_2) \right) \delta_i(x_0),
\]

where \(0 \leq u, v < 2^{n+m'}, v = \beta \cdot 2^n + j\) for \(0 \leq \beta < 2^n\) and \(0 \leq j < 2^n\).

We omit the proof of Theorem 11, which is similar to the proof of Theorem 9 by applying Lemma 9. Moreover, formula (66) shows new constructions of CCCs and CSSs by GBFs, and Theorem 11 can be used to provide a better PMEPR bound.

**Corollary 8:** Let \(\{f_1(x_1)\}_{0 \leq i < 2^{n+m'}}\) and \(\{f_2(x_2)\}_{0 \leq i < 2^n}\) be two CASs of size \(2^{n+m'}\) and \(2^n\), respectively. Then we have GBFs

\[
f(x_0, x_1, x_2) = \sum_{i=0}^{2^{n-1}} (f_1(x_1) + f_2(x_2)) \delta_i(x_0)
\]

is an array of size \(2^n \times 2 \times 2 \times \cdots \times 2\) lying in a CAS of size \(2^{n+m'+2^n}\). Moreover, the sequences evaluated by GBFs \(\pi \cdot f(x_0, x_1, x_2) + f'(x_0, x_1, x_2)\) lies in CSSs of size \(2^{n+m'+2^n}\), where \(\pi\) is a permutation of Boolean variables \((x_0, x_1, x_2)\) and \(f'(x_0, x_1, x_2)\) is an affine GBF.
Example 15: It is experimentally shown in [33, Section VII], the PMEPR of the sequences evaluated by first order Reed-Muller coset of Boolean function
\[
f(x_0, x_1, x_2, x_3, x_4) = x_0 x_1 + x_0 x_4 + x_1 x_4 + x_2 x_4 + x_3 x_4
\]
equals to 3.449. However the results in [33] can only show that the PMEPR is bounded by 8, since it lies in a CSS of size 8. Note that an explanation of this example has been given in [6]. Here we illustrate the function \(f(x_0, x_1, x_2, x_3, x_4)\) lies in a CAS of size 4 by applying Corollary 8.

Let \(n = 2, n' = 0, f_{i}^{(3)} = 0\) for \(1 \leq i \leq 3\), and \(f_{i}^{(1)}\) be given as follows.

\[
\begin{align*}
\{f_{0}^{(1)}(x_1, x_3, x_4)\} &= x_1 x_4 + x_3 x_4, \\
\{f_{1}^{(1)}(x_1, x_3, x_4)\} &= x_1 x_4 + x_3 x_4 + x_1 + x_4, \\
\{f_{2}^{(1)}(x_1, x_3, x_4)\} &= x_1 x_4 + x_3 x_4 + x_4, \\
\{f_{3}^{(1)}(x_1, x_3, x_4)\} &= x_1 x_4 + x_3 x_4 + x_1.
\end{align*}
\]

It is obvious that \(\{f_{0}^{(1)}, f_{3}^{(1)}\}\) and \(\{f_{1}^{(1)}, f_{2}^{(1)}\}\) are both GAPs. So \(\{f_{0}^{(1)}, f_{1}^{(1)}, f_{2}^{(1)}, f_{3}^{(1)}\}\) lies in a CAS of size 4. Then it is easy to check

\[
f(x_0, x_1, x_2, x_3, x_4) = \sum_{i=0}^{3} f_{i}^{(1)}(x_1, x_3, x_4) \delta_{i}(x_0, x_2),
\]

so \(f(x_0, x_1, x_2, x_3, x_4)\) lies in a CAS of size 4 by Corollary 8 and the PMEPR of the sequences evaluated by the first order Reed-Muller coset of this Boolean function is bounded by 4.

VIII. CONCLUDING REMARKS

In this paper, we present a state-of-the-art method to construct CSSs and CCCs by PU matrices, which can be divided into three steps:

1. Construct a desired PU matrix \(U(z)\);
2. Extract the corresponding function matrix \(\tilde{U}(x)\);
3. Construct CCAs, CASs, CSSs and CCCs according to Theorem 1.

The results in this paper are summarized in Figure 3. Our proposed approach not only constructs a large number of new CSSs and CCCs with explicit function forms, but also explains GBF-based constructions in the literature, i.e., they all can be considered as a special case of our constructions. Especially, the well known Golay sequences shown in [10] can be extracted from the seed PU matrices of order 2, and the constructions of CSSs and CCCs with explicit GBFs in [33], [38], [42] can also be obtained by the recursive formula only involving the seed PU matrices of order 2. Although we did not explicitly show the constructions in [6], [7], [54], they can be obtained by the recursive formula only involving the seed PU matrices of order 2 as well. This observation makes the functions derived from (generalized) seed PU matrices of order \(N > 2\) very interesting.

On the other hand, we propose a systematic approach to extract the explicit forms of the functions from the seed PU matrices, which is a key contribution of this paper. The general form of these functions only depends on a basis of functions from \(\mathbb{Z}_N\) to \(\mathbb{Z}_q\) and representatives in the equivalent class of phase BH matrices. Furthermore, we proved that the sequences extracted from the seed PU matrices must fill up a large number of cosets of a linear code. For \(N = q = 3\), the ternary complementary sequences in CSSs of size 3, constructed from the seed PU matrices of order 3, are never reported before. Moreover, most quaternary complementary sequences of size 4 constructed here are novel. We would like to elaborate this more. The inspired narrative for the new sequences extracted from seed PU matrices of order 4 can be explained as follows.

There is only one representative for binary BH matrices of order 4 which is the WHT matrix, while there are two representatives for quaternary BH matrices: the WHT matrix and the DFT matrix. We observe that the known construction of CSSs reported in the literature are extracted from the PU matrices where only the equivalent class of the WHT matrices are involved. Note that WHT matrix of order 4 can be generated by the Kronecker product of the WHT matrix of order 2. So these sequences can also be produced by the recursive formula by the seed PU matrices of order 2. On the other hand, even if there is only one BH matrix which is equivalent to a DFT matrix in the seed PU matrices of order 4, any sequences (with PMEPR upper bounded by 4) extracted from such a seed PU matrix are new.

Note that there are 15 equivalent classes of BH matrices in \(H(4,8)\), and 319 equivalent classes of BH matrices in \(H(4,12)\) [30]. Thus, the results for the seed PU matrices of order \(N\), combined with the recursive formula in Subsection VII-C, may significantly increase the number of the polyphase sequences (with PMEPR upper bounded by \(N\)).

The open problem given in [49] has influenced the field of constructing new CSSs and CCCs for almost 5 decades, i.e., Obtain direct construction procedures for complementary sets with given parameters, namely, the number of sequences in the set and their lengths. From the PU-matrix-based construction in [9], [29], [46], the binary CSSs constructed in [49] by Hadamard matrices are a subset of the CSSs derived from our seed PU matrices. It is stated that the results in [33] provide a partial solution to this open problem. Nevertheless, the results in this paper present a much more deeply nailed down solution to this open problem.

We now pay attention back to the functions derived from seed PU matrices, which contain two components for each function. One component is the \(\delta\)-linear term \(\delta_{L}(q,N)\) which can be easily obtained. However, we need to calculate the second component, i.e., a subset of \(\delta\)-distinct quadratic term \(S_{Q}(q,N)\) intensely. Note that the numbers of \(X_{L}\) and \(\chi_{R}\) which are permutations of symbols \(\{0,1,\cdots,N-1\}\), are both equal to \(N!\). Thus, the computation complexity of the \(\delta\)-quadratic terms is about \((N!)^{2}\) from only one representative of BH matrices. Is it possible to find a general explicit GBF form derived from seed PU matrices for specified BH matrices? Currently, we are able to obtain the sequences derived from the generalized seed PU matrices for DFT matrices and WHT matrices, and prove that inequivalent BH matrices must produce \(\delta\)-distinct quadratic terms, which will be presented in a separate work [53]. Surprisingly we discover an extremely fascinating hidden connection between the sequences in CSSs
and CCCs and the sequences with 2-level autocorrelation, through the trace function and permutation polynomials.

From our recursive framework, binary and quaternary sequences in CSSs of order 4 are determined by the generalized seed PU matrices of order 2 and 4. The GBFs extracted from the generalize seed PU matrices of order 2 and 4 have been explicitly given case by case. A question we ask is whether there is a general form which contains all (or a large subset of) binary and quaternary sequences in the CSSs of order 4 from the recursive constructions in this paper. There are more interesting questions that we could ask by exploring those new constructions presented in this paper. Here, we just list a few.

**APPENDIX A**

**PROOF OF LEMMA 9**

According to formula (16), the generating matrices \( A(z_1) \) and \( B(z_2) \) can be expanded in the form:

\[
A(z_1) = \sum_{x_1} A(x_1) \cdot z_1^{x_1}
\]

and

\[
B(z_2) = \sum_{x_2} B(x_2) \cdot z_2^{x_2},
\]

where \( A_{i,j}(x_1) = \omega^{a_{i,j}(x_1)} \) and \( B_{i,j}(x_2) = \omega^{b_{i,j}(x_2)} \), respectively, for \( 0 \leq i, j < N \). The generalized delay matrix \( D(z_0) \) can be expressed in the form

\[
D(z_0) = \sum_{i=0}^{N-1} E_i \cdot \phi_i(z_0) = \sum_{i=0}^{N-1} E_i \cdot z_0^{x_0},
\]

where \( i = \sum_{i=0}^{n-1} x_i \cdot 2^n \). Then we have

\[
C(z_0, z_1, z_2) = A(z_1) \cdot D(z_0) \cdot B(z_2) = \left( \sum_{x_1} A(x_1) \cdot z_1^{x_1} \right) \left( \sum_{i=0}^{N-1} E_i \cdot z_0^{x_0} \right) \cdot \left( \sum_{x_2} B(x_2) \cdot z_2^{x_2} \right) = \sum_{x_0, x_1, x_2} A(x_1) \cdot E_i \cdot B(x_2) \cdot z_0^{x_0} z_1^{x_1} z_2^{x_2}.
\]

Suppose that \( C(x_0, x_1, x_2) = A(x_1) \cdot E_i \cdot B(x_2) \). Then the entries of \( C(x_0, x_1, x_2) \) can be expressed by

\[
C_{r,s}(x_0, x_1, x_2) = A_{r,s}(x_1) B_{r,s}(x_2) = \omega^{a_{r,s}(x_1) + b_{r,s}(x_2)}.
\]

From the definition of the Kronecker-delta function \( \delta_i \), we have

\[
a_{r,s}(x_1) + b_{r,s}(x_2) = \sum_{i=0}^{N-1} a_{r,i}(x_1) \delta_i(x_0) + \sum_{i=0}^{N-1} b_{i,s}(x_2) \delta_i(x_0),
\]

which is a GBF (array) from \( \mathbb{Z}_q^{n+m_1+m_2} \) to \( \mathbb{Z}_q \), denoted by \( c_{r,s}(x_0, x_1, x_2) \). Let \( C(x_0, x_1, x_2) \) be the function matrix with entry \( c_{r,s}(x_0, x_1, x_2) \) at position \( (r, s) \). Then \( C(z_0, z_1, z_2) \) is the generating matrix of \( C(x_0, x_1, x_2) \), which completes the proof.

**APPENDIX B**

**PROOF OF THEOREM 8**

It is obvious that \( G(z) \) is a PU matrix. From Definition 15, we know that the entries of the permutation matrix \( P \) equals to 1 at position \((j, 2j)\) and \((j + 2^n, 2j + 1)\) for \( 0 \leq j < 2^n \). Let \( A \) and \( B \) be two matrices of order \( 2^{n+1} \) such that
\[ B = P A P^T. \] Then the entries \( B_{i,j} = A_{2j,2j}, B_{j,j} = A_{2j+1,2j+1}, B_{j+1,j} = A_{2j+2,2j+1}, \) and \( B_{j,j+1} = A_{2j+1,2j+2} \). We have
\[
P = \begin{bmatrix}
  U^{(0)}(z) & 0 & \cdots & 0 \\
  0 & U^{(1)}(z) & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \cdots & U^{(2n-1)}(z)
\end{bmatrix}
\]
\[
P^T = \begin{bmatrix}
  V_{0,0}(z) & V_{0,1}(z) \\
  V_{1,0}(z) & V_{1,1}(z)
\end{bmatrix}
\]
where \( V_{\alpha,\beta}(z) \) (\( 0 \leq \alpha, \beta \leq 1 \)) is a diagonal matrix given by
\[
V_{\alpha,\beta}(z) = \text{diag}(U^{(0)}_{\alpha,\beta}(z), U^{(1)}_{\alpha,\beta}(z), \ldots, U^{(2n-1)}_{\alpha,\beta}(z)).
\]
Note that \( U^{(j)}_{\alpha,\beta}(z) \) is the generating function of the GBF
\[
f^{(j)}(x) = \frac{q}{2} \alpha x^{\sigma_j} + \frac{q}{2} \beta x^{\sigma_j(m-1)}
\]
for \( 0 \leq j < 2^n \).

The multivariate polynomial matrix \( G(x) \) can be represented by a block matrix
\[
G(z) = \begin{bmatrix}
  G_{0,0}(z) & G_{0,1}(z) \\
  G_{1,0}(z) & G_{1,1}(z)
\end{bmatrix}.
\]

On the other hand, we have
\[
G(z) = \begin{bmatrix}
  H^{(0)} & 0 \\
  0 & H^{(1)}
\end{bmatrix}
\begin{bmatrix}
  V_{0,0}(z) & V_{0,1}(z) \\
  V_{1,0}(z) & V_{1,1}(z)
\end{bmatrix}
\]
\[
\begin{bmatrix}
  H^{(0)} & 0 \\
  0 & H^{(1)}
\end{bmatrix}
\begin{bmatrix}
  V_{0,0}(z) & V_{0,1}(z) \\
  V_{1,0}(z) & V_{1,1}(z)
\end{bmatrix}
\]
Then each block matrix can be represented by
\[
G_{\alpha,\beta}(z) = H^{(\alpha)} V_{\alpha,\beta}(z)
\]
and each entry of \( G(z) \) can be given by
\[
G_{u,v}(z) = H_{i,j}^{(\alpha)} U^{(j)}_{\alpha,\beta}(z),
\]
which is the generating function of the GBF
\[
\tilde{G}_{u,v}(x) = f^{(j)}(x) = \frac{q}{2} \alpha x^{\sigma_j} + \frac{q}{2} \beta x^{\sigma_j(m-1)}
\]
where \( u = \alpha \cdot 2^n + i \) and \( v = \beta \cdot 2^n + j \) for \( 0 \leq \alpha, \beta \leq 1 \) and \( 0 \leq i, j < 2^n \). Thus the assertion is established.

**APPENDIX C**

**Proof of Theorem 9**

It is obvious that \( M(z_0, z_1) \) is a PU matrix. The multivariate polynomial matrices \( G(z_1) \) and \( M(z_0, z_1) \) can be interpreted by block matrices
\[
G(z_0) = \begin{bmatrix}
  G_{0,0}(z_0) & G_{0,1}(z_0) \\
  G_{1,0}(z_0) & G_{1,1}(z_0)
\end{bmatrix}
\]
and
\[
M(z_0, z_1) = \begin{bmatrix}
  M_{0,0}(z_0, z_1) & M_{0,1}(z_0, z_1) \\
  M_{1,0}(z_0, z_1) & M_{1,1}(z_0, z_1)
\end{bmatrix}
\]
respectively. From the definition, we have
\[
M(z_0, z_1) = \begin{bmatrix}
  G_{0,0}(z_0) & G_{0,1}(z_0) \\
  G_{1,0}(z_0) & G_{1,1}(z_0)
\end{bmatrix}
\begin{bmatrix}
  D(z_1) & 0 \\
  0 & D(z_1)
\end{bmatrix}
\begin{bmatrix}
  H^{(2)} & 0 \\
  0 & H^{(3)}
\end{bmatrix}
\]
\[
= \begin{bmatrix}
  G_{0,0}(z_0) D(z_1) H^{(2)} & G_{0,1}(z_0) D(z_1) H^{(3)} \\
  G_{1,0}(z_0) D(z_1) H^{(2)} & G_{1,1}(z_0) D(z_1) H^{(3)}
\end{bmatrix},
\]
which imply
\[
M_{\alpha,\beta}(z_0, z_1) = G_{\alpha,\beta}(z_0) D(z_1) H^{(\beta+2)}
\]
for \( 0 \leq \alpha, \beta \leq 1 \).

According to Lemma 9, we have
\[
\tilde{M}_{\alpha,\beta}^{2n+i,\beta,2n+j}(x_0, x_1)
\]
\[
= \sum_{i=0}^{2^n-1} \left( G_{\alpha,\beta}^{2n+i,\beta,2n+i}(x_0) + H^{(\beta+2)}_{i,j} \right) \delta_i(x_1),
\]
which completes the proof by substituting (53) into the above formula.

**ACKNOWLEDGMENT**

The first author wishes to thank Dr. K.-U. Schmidt for his valuable discussions of the known constructions of complementary sets in [6], [7], [42], [44] when the author presented that the new CSSs were constructed in SETA 2016 [52].

The authors wish to thank Dr. S. Z. Budišin for his valuable suggestions on the enumeration of sequences in Corollary 3 and the general constructions in Subsection VII-C.

The work was partially done when Dongxu Ma was an exchange Ph.D. student during September 2016–August 2018 and Zilong Wang was a visiting professor during February 2020–January 2021, at the Department of Electrical and Computer Engineering (ECE), University of Waterloo, Canada. Erzhong Xue is currently with ECE, UW, as an exchange Ph.D. student from April 2021–March 2022.

**REFERENCES**

[1] S. Z. Budisić and P. Spasojević, “Filter bank representation of complementary sequence pairs,” in Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton), Champaign, IL, USA: Univ. of Illinois at Urbana-Champaign, Oct. 2012.

[2] S. Z. Budisić and P. Spasojević, “Paranitary generation/correlation of QAM complementary sequence pairs,” Cryptogr. Commun., vol. 6, no. 1, pp. 59–102, Mar. 2014.

[3] S. Z. Budisić and P. Spasojević, “Paranitary-based Boolean generator for QAM sequences of length 2^K,” IEEE Trans. Inf. Theory, vol. 64, no. 8, pp. 9538–9563, Aug. 2018.

[4] S. Z. Budisić, “A radix-M construction for complementary sets,” 2018, arXiv:1808.10400 [Online]. Available: http://arxiv.org/abs/1808.10400.

[5] A. Butson, “Generalized Hadamard matrices,” Proc. Amer. Math. Soc., vol. 13, no. 6, pp. 894–898, 1962.

[6] C.-Y. Chen, C.-H. Wang, and C.-C. Chao, “Complementary sets and Reed-Muller codes for peak-to-average power ratio reduction in OFDM,” in Proc. 16th AAECC Symp., in Lecture Notes Comput. Science, vol. 3857, 2006, pp. 317–327.

[7] 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, Nov. 2008.

[8] C. V. Chong, R. Venkataaramani, and V. Tarokh, “A new construction of 16-QAM Golay complementary sequences,” IEEE Trans. Inf. Theory, vol. 49, no. 11, pp. 2953–2959, Nov. 2003.

[9] S. Das, S. Budisić, S. Majhi, Z. Liu, and Y. L. Guan, “A multiplier-free generator for polyphase complementary code sets,” IEEE Trans. Signal Process., vol. 66, no. 5, pp. 1184–1196, Mar. 2018.

[10] 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.

[11] X. Deng and P. Fan, “Spreading sequence sets with zero correlation zone,” Electron. Lett., vol. 36, no. 11, pp. 993–994, May 2000.

[12] J. Ding, M. Noshad, and V. Tarokh, “Complementary lattice arrays for coded aperture imaging,” J. Opt. Soc. Amer. A, Opt. Image Sci., vol. 33, no. 5, pp. 863–881, 2016.

[13] F. Fiedler and J. Jedwab, “How do more Golay sequences arise?” IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4261–4266, Sep. 2006.
[49] C. RoBing and V. Tarokh, “A construction of OFDM 16-QAM sequences having low peak powers,” IEEE Trans. Inf. Theory, vol. 47, no. 5, pp. 2091–2094, Jul. 2001.

[50] K.-U. Schmidt, “On cosets of the generalized first-order Reed-Muller code with low PMEPR,” IEEE Trans. Inf. Theory, vol. 52, no. 7, pp. 3220–3232, Jul. 2006.

[51] K.-U. Schmidt, “Complementary sets, generalized Reed-Muller codes, and power control for OFDM,” IEEE Trans. Inf. Theory, vol. 53, no. 2, pp. 808–814, Feb. 2007.

[52] L. Serge, Graduate Texts in Mathematics: Algebra. New York, NY, USA: Springer, 2002.

[53] T. E. Stinchcombe, “Aperiodic autocorrelations of length 2^m sequences, complementarity, and power control for OFDM,” Ph.D. dissertation, Dept. Math., Univ. London, London, U.K., 2000.

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

[55] V. Tarokh and H. Jafarkhani, “On the computation and reduction of the peak-to-average power ratio in multicarrier communications,” IEEE Trans. Commun., vol. 48, no. 1, pp. 37–44, Jan. 2000.

[56] B. Tarokh and H. R. Sadjadpour, “Construction of OFDM M-QAM sequences with low peak-to-average power ratio,” IEEE Trans. Commun., vol. 51, no. 1, pp. 25–28, Jan. 2003.

[57] C.-C. Tseng and C. Liu, “Complementary sets of sequences,” IEEE Trans. Inf. Theory, vol. IT-18, no. 5, pp. 644–652, Sep. 1972.

[58] Z. Wang, G. Gong, and R. Feng, “A generalized construction of OFDM M-QAM sequences with low peak-to-average power ratio,” Adv. Math. Commun., vol. 3, no. 4, pp. 421–428, 2009.

[59] Z. Wang, M. Parker, G. Gong, and G. Wu, “On the PMEPR of the binary Golay sequences of length 2^n,” IEEE Trans. Inf. Theory, vol. 60, no. 4, pp. 2391–2398, Apr. 2014.

[60] D. Ma, Z. Wang, G. Gong, and H. Li, “A new method to construct Golay complementary set and near-complementary set by parametric matrices,” in Proc. 8th Int. Workshop Signal Design Appl. Commun. (IWSDA), Chengdu, China, Sep. 2017, pp. 252–263.

[61] Z. Wang and G. Gong, “Constructions of complementary sequence sets and complete complementary codes by 2-level autocorrelation sequences and permutation polynomials,” 2020, arXiv:2005.05825. [Online]. Available: http://arxiv.org/abs/2005.05825.

[62] G. Wu, Y. Zhang, and X. Liu, “New complementary sets of length 2^m and size 4,” Adv. Math. Commun., vol. 10, no. 4, pp. 825–845, 2016.
Guang Gong (Fellow, IEEE) received the B.S. degree in mathematics from Xichang Normal College in 1981, the M.S. degree in applied mathematics from Xidian University in 1985, and the Ph.D. degree in electrical engineering from the University of Electronic Science and Technology of China (UESTC) in 1990. She was promoted to the position of an Associate Professor at UESTC in 1993. From 1996 to 1998, she worked with Dr. Solomon W. Golomb with the University of Southern California and joined the University of Waterloo, Canada, in 1998, as an Associate Professor with the Department of Electrical and Computer Engineering in 2000, and a Full Professor in 2004. She has authored or coauthored more than 360 technical articles, two books, and two patents. Her research interests are in the areas of pseudorandom generation, cryptography, and communication security. Her current research focuses on pseudorandom generation, lightweight cryptography (LWC), the IoT security, blockchain privacy, and privacy preserving machine learning.

Dr. Gong has received several awards, including the Premier’s Research Excellence Award, Canada, in 2001, the Ontario Research Fund—Research Excellence Award, Canada, in 2010, and the University Research Chair in 2018. She has served on numerous technical program committees and conferences as the co-chair/an organizer or a committee member. She has been serving/served as an Associate Editor for several journals, including the IEEE TRANSACTIONS ON INFORMATION THEORY from 2005 to 2008, from 2017 to 2018, and since 2020, and CRYPTOGRAPHY AND COMMUNICATIONS since 2007. Her research is supported by government grant agencies as well as industrial grants. She received a Post-Doctoral Fellowship from the Fondazione Ugo Bordoni, Rome, Italy.

Erzhong Xue received the B.E. degree from Xidian University, China, in 2016, where he is currently pursuing the Ph.D. degree. He has been with the Department of Electrical and Computer Engineering, University of Waterloo, as an Exchange Ph.D. Student during April 2021–March 2022. His research interests are in the areas of sequence design, information security, and cryptography.