Construction of New Optimal Z-Complementary Code Sets from Z-Paraunitary Matrices

Shibsankar Das*, **Udaya Parampalli**[⋆], **Sudhan Majhi**[†], **and Zilong Liu**[‡]

*Department of Mathematics, Indian Institute of Technology Patna, Bihar, India
[⋆]School of Computing and Information Systems, University of Melbourne, Victoria, Australia
[†]Department of Electrical Engineering, Indian Institute of Technology Patna, Bihar, India
[‡]Institute for Communication Systems, 5G Innovation Centre, University of Surrey, U.K.
Email:{shibsankar.pma15}@iitp.ac.in

Abstract—**In this paper, we first introduce a novel concept, called Z-paraunitary (ZPU) matrices. These ZPU matrices include conventional PU matrices as a special case. Then, we show that there exists an equivalence between a ZPU matrix and a Z-complementary code set (ZCCS) when the latter is expressed as a matrix with polynomial entries. The proposed ZPU matrix has an advantage over the conventional PU matrix with regard to the availability of wider range of matrix sizes and sequence lengths. In addition, the proposed construction framework can accommodate more choices of ZCCS parameters compared to the existing works.**

Index Terms—**Paraunitary Matrices, Z-Paraunitary Matrices, Z-Complementary Sequences, Unimodular Sequences.**

I. INTRODUCTION

A matrix of polynomials is simply a matrix whose entries are polynomials. The matrices of polynomials have many potential applications in the control theory [1] and filter bank theory [2], but in recent years they have been applied in the area of complementary sequence design [3], [4]. A paraunitary (PU) matrix refers to a matrix of polynomials over the indeterminate variable z^{-1} which is unitary on the unit circle. The concept of PU matrices was introduced by Vaidyanathan [2] in the theory of filter-banks. The past few decades have witnessed that a family of PU matrices has been one of the key tools in the area of filter-bank theory [5], wireless communication [6], [7], cryptography [8], and so on. In [6], it has been shown that a binary PU precoded OFDM system has better error probability performance than the conventional OFDM systems. Subsequently, the application of PU matrix has been extended to MIMO-OFDM system [9]. The precoding applications of PU matrices can also be found in CDMA systems [7].

In [2], it is shown that any arbitrary PU matrix can be factorized into a product of unitary and diagonal matrices. This factorization is said to be an expanded product form of a PU matrix. Thus, the size of PU matrix is limited by the existence of unitary matrices for the given number of phases. For example, a 6×6 binary PU matrix does not exist since a binary unitary matrix of size 6×6 does not exist. Note that a binary PU matrix also refers to an antipodal PU (APU) matrix. In [6], Phoong and Chang have pointed out that it is still unclear if there exist APU matrices with odd length ≥ 3 and APU matrices with dimensions of $4k + 2$, for $k \geq 1$. Moreover, an $M \times K$ PU matrix does not exist when $K > M$, which may limit their applications in the field of signal processing.

Recently, PU matrix has received very wide interest in the area of complementary sequence design [3], [10]-[17]. In [3], a compact formulation has been proposed for complementary sequence pairs (and sets) by using PU matrices. The applications of PU matrices have also been extended to q-ary complementary sequence sets [10], and QAM complementary sequence sets [13]. Note that [10] introduced the use of Butson-type Hadamard (BH) matrices in the PU method to the construction of complementary sequences. In [16], it is explicitly shown that there exists an equivalence between a square PU matrix and complete complementary codes (CCC) when it is expressed as a matrix with polynomial entries. In [17], a compact formulation for designing polyphase CCC with various sequence lengths has been reported. Very recently, the applications of PU matrices have been extended to the construction of zero correlation zone (ZCZ) sequence sets [18].

A limitation of CCC is that the set size is equal to the number of constituent sequences (i.e., the flock size) in each set, which restricts their applications to support more users. It is worth mentioning that the complexity in a MC-CDMA system increases exponentially with the flock size. To overcome this weakness, Z-complementary code sets (ZCCS) are introduced by Fan *et al.* [19], where Z denotes the ZCZ width. In the literature, Z-complementary sequences are also investigated in [20]-[24]. Most recently, direct constructions based on generalized Boolean functions have been explored in [25] and [26]. There is another type of code known as inter-group complementary code set [27] which can be considered as a special case of ZCCS.

In this paper, we introduce the idea of Z-paraunitary (ZPU) matrix which includes conventional PU matrix as a special case. The key idea is to relax the condition on the range of time-shifts of interest to $Z \leq L$. This allows us to show there exists a one-to-one correspondence between a ZPU matrix and ZCCS when the matrix has sequences as its entries. Moreover, this paper proposes a compact formulation of optimal ZCCSs described in z-domain framework. Therefore, the matrix sizes and sequence lengths of ZPU matrices are more flexible compared to conventional PU matrices.

II. PRELIMINARIES

In this section, we will present some basic definitions, notations and preliminaries.

A. Notations

- The z-transform of aperiodic cross-correlation function (ACCF) $R_{\boldsymbol{x},\boldsymbol{y}}[\tau]$ between two length-L complex-valued sequences $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined by $R_{\boldsymbol{x},\boldsymbol{y}}(z) = \sum_{\tau=-(L-1)}^{L-1} R_{\boldsymbol{x},\boldsymbol{y}}[\tau] \cdot z^{-\tau} = x(z) \cdot y^{*}\left(z^{-1}\right)$, where $(\cdot)^{*}$ denotes complex conjugate (see [12]). Since $R_{\boldsymbol{x},\boldsymbol{y}}[-\tau] = R^{*}_{\boldsymbol{y},\boldsymbol{x}}[\tau]$, it is sufficient to calculate the ACCF $R_{\boldsymbol{x},\boldsymbol{y}}[\tau]$ only for $0 \leq \tau < L$.
- The zero correlation zone (ZCZ) is denoted by the upper case Z (not to be confused with the indeterminate variable z in z-transform).
- The least common multiple between numbers is denoted by LCM.
- For an $M \times K$ matrix $\mathbf{X}(z)$ of polynomials over z^{-1}, the tilde operator is defined by $\widetilde{\mathbf{X}(z)} = \mathbf{X}^{H}\left(z^{-1}\right)$, where H is the Hermitian operation.
- The Butson-type Hadamard matrix $BH(M, q)$ refers to a complex Hadamard matrix of size $M \times M$ with q^{th} roots of unity entries [28]. $BH(M, 2)$ represents a binary Hadamard matrix denoted by $\mathbf{H}_M$ for $M = 2, 4m$ and $BH(M, M)$ represents discrete Fourier transform (DFT) matrix denoted by $\mathbf{F}_M$.

Let $\mathbf{X}(z) = \left[\mathbf{x}_0(z), \mathbf{x}_1(z), \cdots, \mathbf{x}_{K-1}(z)\right]$ be a polynomial matrix of K column vectors, each of size M, i.e.,

$$\mathbf{x}_{\mu}(z) = \left[x_{0\mu}(z), x_{1\mu}(z), \cdots, x_{(M-1)\mu}(z)\right]^{T}, \quad (1)$$

where $0 \leqslant \mu \leqslant K-1$ and $x_{m\mu}(z)$ is a polynomial of complex numbers coefficients and degree $L-1$ for each $m \in \{0, 1, \cdots, M-1\}$. The z-transform of ACCF sum $S_{\mathbf{x}_{\mu},\mathbf{x}_{\nu}}[\tau]$ between two columns $\mathbf{x}_{\mu}(z)$ and $\mathbf{x}_{\nu}(z)$ $(0 \leq \mu, \nu \leq M-1)$ is given by

$$S_{\mathbf{x}_{\mu},\mathbf{x}_{\nu}}(z) = \sum_{m=0}^{M-1} R_{\boldsymbol{x}_{m\mu},\boldsymbol{x}_{m\nu}}(z). \quad (2)$$

From z-transform of ACCF sum given by (2) and the tilde operation, the product $\widetilde{\mathbf{X}(z)} \cdot \mathbf{X}(z)$ of matrices can be expressed as

$$\widetilde{\mathbf{X}(z)} \cdot \mathbf{X}(z) = \left[S_{\mathbf{x}_{\mu},\mathbf{x}_{\nu}}(z)\right]_{K \times K}. \quad (3)$$

***Remark** 1:* Note that the matrix $\widetilde{\mathbf{X}(z)} \cdot \mathbf{X}(z)$ can be expressed only by the z-transforms of AACF sums and ACCF sums between sequence sets. We call it as the matrix of ACCF sums.

B. Paraunitary (PU) Matrix

A PU matrix is a matrix of polynomials over z^{-1} which is unitary on the unit circle, i.e., $|z| = 1$.

***Definition** 1:* An $M \times K$ polynomial matrix $\mathbf{X}(z)$ is said to be a PU matrix if the following identity holds:

$$\widetilde{\mathbf{X}(z)} \cdot \mathbf{X}(z) = c \cdot \mathbf{I}_K, \quad (4)$$

where $\mathbf{I}_K$ is the identity matrix of size $K \times K$ and c is a positive constant.

Equivalently, the above condition (4) can be written by

$$S_{\mathbf{x}_{\mu},\mathbf{x}_{\nu}}(z) = c \cdot \delta(\mu - \nu), \quad (5)$$

where δ denotes the delta function. Clearly, the matrix $\mathbf{X}(z)$ satisfies the ideal correlation properties over the whole range of time-shift $Z = L$. The degree of a PU matrix refers to the minimum number of delays required to implement it. The length of a PU matrix refers to the length of the constituent sequences. A PU matrix is called a unimodular PU matrix if it has only unimodular coefficients. For example, a PU matrix with ± 1 coefficients refers to a binary PU matrix.

We give one example of a binary PU matrix.

***Example** 1:* Let $M = K = 2$. A 2×2 binary PU matrix $\mathbf{X}(z)$ with sequence length $L = 4$ is given by

$$\mathbf{X}(z) = \begin{bmatrix} 1 + z^{-1} + z^{-2} - z^{-3} & 1 + z^{-1} - z^{-2} + z^{-3} \\ 1 - z^{-1} + z^{-2} + z^{-3} & 1 - z^{-1} - z^{-2} - z^{-3} \end{bmatrix}_{2 \times 2}. \quad (6)$$

It is easy to verify that $S_{\mathbf{x}_{\mu},\mathbf{x}_{\nu}}(z) = 8 \cdot \delta(\mu - \nu)$, $\mu, \nu = 0, 1$. Therefore, the matrix of ACCF sums is given by

$$\widetilde{\mathbf{X}(z)} \cdot \mathbf{X}(z) = \begin{bmatrix} S_{\mathbf{x}_0,\mathbf{x}_0}(z) & S_{\mathbf{x}_0,\mathbf{x}_1}(z) \\ S_{\mathbf{x}_1,\mathbf{x}_0}(z) & S_{\mathbf{x}_1,\mathbf{x}_1}(z) \end{bmatrix} = 8 \cdot \mathbf{I}_2, \quad (7)$$

where $S_{\mathbf{x}_0,\mathbf{x}_0}(z) = S_{\mathbf{x}_1,\mathbf{x}_1}(z) = 8 + 0z^{-1} + 0z^{-2} + 0z^{-3}$ and $S_{\mathbf{x}_0,\mathbf{x}_1}(z) = S_{\mathbf{x}_1,\mathbf{x}_0}(z) = 0 + 0z^{-1} + 0z^{-2} + 0z^{-3}$. Note that the ZCZ width for this matrix is over the whole range of time-shifts $Z = L = 4$.

For an $M \times K$ PU matrix, we have the following relationship between M and K.

***Result** 1 ([2]):* For any arbitrary $M \times K$ PU matrix, the following inequality is true:

$$K \leq M. \quad (8)$$

By using *Result 1*, we can say that an $M \times K$ PU matrix does not exist when $K > M$. Later, we will show that an $M \times K$ ZPU matrix exists when K can be much larger than M. Also, binary ZPU matrices with odd lengths ≥ 3 exist.

C. Z-Complementary Code Sets (ZCCS)

A set $\mathbf{x}(z)$ of M sequences with equal length L is called a Z-complementary code (ZCC) [19] if

$$S_{\mathbf{x}}(z) = ML + \sum_{\tau=Z}^{L-1} S_{\mathbf{x}}[\tau] \cdot z^{-\tau}, \quad (9)$$

where Z denotes the zero correlation zone (ZCZ). When $Z = L$, ZCC refers to a conventional complementary set of sequences. A ZCC $\mathbf{y}(z)$ of M sequences with equal length L is said to be a Z-complementary mate of ZCC $\mathbf{x}(z)$ if

$$S_{\mathbf{x},\mathbf{y}}(z) = 0 + \sum_{\tau=Z}^{L-1} S_{\mathbf{x},\mathbf{y}}[\tau] \cdot z^{-\tau}. \quad (10)$$

Clearly, Z-complementary mate becomes a conventional complementary mate when $Z = L$. For a given ZCC of size M, there exist more than M distinct Z-complementary mates. Note that we are interested only to calculate the ACCF sum for the time-shifts $0 \leq \tau < L$ due to the symmetry.

***Definition** 2:* The family $\mathbf{X}(z)$ is called a Z-complementary code sets (ZCCS) if each set is ZCC and two distinct sets are Z-complementary mates.
We denote it as (K,Z)-ZCCS$_M^L$. Obviously, (K,Z)-ZCCS$_M^L$ becomes a conventional mutually orthogonal complementary sets of sequences when $Z=L$. A (K,Z)-ZCCS$_M^L$ can be regarded as ZCCC when $K=M$. In fact, a (K,Z)-ZCCS$_M^L$ becomes a conventional CCC when $Z=L$ and $K=M$.

For any given (K,Z)-ZCCS$_M^L$, the theoretical upper bound [19], [29] on K is given by

$$K \le M\lfloor L/Z \rfloor, \tag{11}$$

where $\lfloor x \rfloor$ represents the largest integer smaller than or equal to x.

III. CONCEPT OF Z-PARAUNITARY MATRICES

In this section, we first introduce the concept of ZPU matrices. Then, we show the relationship between ZPU matrix and (K,Z)-ZCCS$_M^L$.

A. *Idea of ZPU Matrices*

***Definition** 3:* An $M\times K$ matrix $\mathbf{X}(z)$ of polynomials over z^{-1} is said to be a ZPU matrix if the following relation holds:

$$\begin{aligned}\widetilde{\mathbf{X}(z)}\cdot\mathbf{X}(z) &= \left[S_{\mathbf{x}_\mu,\mathbf{x}_\nu}(z)\right]_{K\times K}\\ &= c\cdot\mathbf{I}_K \text{ within the ZCZ width } Z.\end{aligned} \tag{12}$$

It is worth noting that we are focused on the aperiodic correlation sums between the sets within the zone of length $Z\le L$. The correlation terms within the time-shifts from $-(Z-1)$ to $(Z-1)$ are taken into consideration in the right hand side of (12). By applying (3), an equivalent expression of (12) can be written by

$$S_{\mathbf{x}_\mu,\mathbf{x}_\nu}(z) = c\cdot\delta(\mu-\nu) + \sum_{\tau=Z}^{L-1} S_{\mathbf{x}_\mu,\mathbf{x}_\nu}[\tau]\cdot z^{-\tau}, \tag{13}$$

where Z is the ZCZ width and $0\le\mu,\nu\le K-1$. We call it as ZPU matrix of size $M\times K$, sequence length L (i.e., degree $L-1$), and the ZCZ width Z.

Clearly, *Definition 3* includes *Definition 1* as a special case when $Z=L$. That is, a ZPU matrix becomes a conventional PU matrix when $Z=L$. Similar to a conventional PU matrix, we can define the degree and length for a ZPU matrix. Since unimodular sequences with good correlation properties are of strong interest in digital communications, we are focused on unimodular ZPU matrices throughout this paper.

We give out one example of ZPU matrix to illustrate our new concept.

***Example** 2:* Let $M=K=2$ and $L=3$. A binary polynomial matrix $\mathbf{X}(z)$ of size 2×2 and length $L=3$ is given by

$$\mathbf{X}(z) = \begin{bmatrix} 1+z^{-1}+z^{-2} & 1-z^{-1}+z^{-2}\\ 1-z^{-1}+z^{-2} & -1-z^{-1}-z^{-2}\end{bmatrix}_{2\times 2}. \tag{14}$$

In this case, the ACCF sum between two sets $\mathbf{x}_0(z)$ and $\mathbf{x}_1(z)$ is given by $S_{\mathbf{x}_0,\mathbf{x}_1}(z) = S_{\mathbf{x}_1,\mathbf{x}_0}(z) = 0+0z^{-1}+0z^{-2}$. Also, the AACF sums of $\mathbf{x}_0(z)$ and $\mathbf{x}_1(z)$ are given by $S_{\mathbf{x}_0,\mathbf{x}_0}(z) = S_{\mathbf{x}_1,\mathbf{x}_1}(z) = 6+0z^{-1}+2z^{-2}$. Thus, the matrix of ACCF sums becomes

$$\begin{aligned}\widetilde{\mathbf{X}(z)}\cdot\mathbf{X}(z) &= \begin{bmatrix} S_{\mathbf{x}_0,\mathbf{x}_0}(z) & S_{\mathbf{x}_0,\mathbf{x}_1}(z)\\ S_{\mathbf{x}_1,\mathbf{x}_0}(z) & S_{\mathbf{x}_1,\mathbf{x}_1}(z)\end{bmatrix}_{2\times 2}\\ &= \begin{bmatrix} 6+0z^{-1}+2z^{-2} & 0+0z^{-1}+0z^{-2}\\ 0+0z^{-1}+0z^{-2} & 6+0z^{-1}+2z^{-2}\end{bmatrix}_{2\times 2}\\ &= 6\cdot\mathbf{I}_2 \text{ within the ZCZ width } 2.\end{aligned} \tag{15}$$

Note that we can omit the terms which are outside of the ZCZ width $Z=2$ in $S_{\mathbf{x}_\mu,\mathbf{x}_\nu}(z)$. Clearly, the condition (12) is satisfied for $Z=2$ and hence $\mathbf{X}(z)$ is a binary 2-PU matrix.

B. *Relationship between ZPU Matrix and ZCCS*

From the definitions of ZPU matrix and ZCCS, we have the following property.

***Property** 1:* A polynomial matrix $\mathbf{X}(z)$ is a ZPU matrix with size $M\times K$ and sequence length L if and only if it is a (K,Z)-ZCCS$_M^L$.

Proof: For any two columns $\mathbf{x}_\mu(z)$ and $\mathbf{x}_\nu(z)$ of $\mathbf{X}(z)$, we can write

$$S_{\mathbf{x}_\mu,\mathbf{x}_\nu}(z) = \sum_{m=0}^{M-1} R_{\boldsymbol{x}_{m\mu},\boldsymbol{x}_{m\nu}}(z), \tag{16}$$

where $\mathbf{x}_\mu(z) = \left[x_{0\mu}(z), x_{1\mu}(z), \cdots, x_{(M-1)\mu}(z)\right]^T$ consisting of M unimodular sequences of equal length L and $0\le\mu,\nu\le K-1$. Then, we have

$$S_{\mathbf{x}_\mu,\mathbf{x}_\nu}(z) = c\cdot\delta(\mu-\nu) + \sum_{\tau=Z}^{L-1} S_{\mathbf{x}_\mu,\mathbf{x}_\nu}[\tau]\cdot z^{-\tau}$$

if and only if $\widetilde{\mathbf{X}(z)}\cdot\mathbf{X}(z) = c\cdot\mathbf{I}_K$ within the ZCZ width Z. Thus, the matrix $\mathbf{X}(z)$ is a ZPU matrix $\Leftrightarrow$ $\widetilde{\mathbf{X}(z)}\cdot\mathbf{X}(z) = c\cdot\mathbf{I}_K$ within the ZCZ width Z $\Leftrightarrow$ $S_{\mathbf{x}_\mu,\mathbf{x}_\nu}(z) = c\cdot\delta(\mu-\nu) + \sum_{\tau=Z}^{L-1} S_{\mathbf{x}_\mu,\mathbf{x}_\nu}[\tau]\cdot z^{-\tau}$ $\Leftrightarrow$ $\mathbf{X}(z)$ is a (K,Z)-ZCCS$_M^L$. This completes the proof. ∎

***Remark** 2:* Based on *Property 1*, we can say that there exists an equivalence between ZCCS and ZPU matrix. This equivalence allows us to find more binary ZPU matrices with odd lengths ≥ 3 compared to the conventional PU matrices.

***Remark** 3:* We observe that *Property 1* includes [16, Th. 1] as a special case when $M=K$ and $Z=L$.

By using *Property 1*, we have the following corollary.

***Corollary** 1:* For an $M\times K$ ZPU matrix, the mathematical upper bound of K is given by

$$K \le M\lfloor L/Z \rfloor. \tag{17}$$

A ZPU matrix is said to be an optimal ZPU matrix if $K=M\lfloor L/Z \rfloor$.

***Remark** 4:* According to *Corollary 1*, K can be much larger than M for an $M\times K$ ZPU matrix. Thus, ZPU matrices have neither limitation on matrix sizes nor limitation on the sequence lengths.

IV. PROPOSED CONSTRUCTION OF OPTIMAL Z-PARAUNITARY MATRICES

In this section, we provide a novel construction of optimal ZPU matrices. It is well known that ZCCSs have potential applications in MC-CDMA system to support more users. Therefore, we are focused on optimal ZPU matrices when K is larger than M.

A. *Proposed Construction*

***Theorem** 1:* Let M and K be two positive integers such that $K = MP$ for some positive integer P. Let $\mathbf{U}_K$ and $\mathbf{U}_M$ be two BH matrices of size $K \times K$ and $M \times M$, respectively. Let us consider a block matrix $\mathbf{G} = \Big[\mathbf{U}_M \ \mathbf{U}_M \ \cdots \ \mathbf{U}_M (P \text{ times})\Big]$. Note that $\mathbf{G}$ is a block matrix of size $M \times K$. Then, a polynomial matrix $\boldsymbol{\mathcal{G}}(z)$ of size $M \times K$ and degree $K-1$ is given by

$$\boldsymbol{\mathcal{G}}(z) = \mathbf{G} \cdot \mathbf{D}_K(z) \cdot \mathbf{U}_K, \tag{18}$$

where $\mathbf{D}_K(z) = \text{diag}\Big(1, z^{-1}, \cdots, z^{-(K-1)}\Big)$. Then, the matrix $\boldsymbol{\mathcal{G}}(z)$ given by (18) is an optimal unimodular ZPU matrix of size $M \times K$, sequence length K and ZCZ width $Z = M$.

Proof: We first show that the sequences generated by (18) are unimodular sequences. Let $\mathbf{G} = [a_{mk}]_{M \times K}$ and $\mathbf{U}_K = [h_{\mu\nu}]_{K \times K}$. Let $\mathbf{a}_k$ be the k-th column vector of the block matrix $\mathbf{G}$. Note that $\mathbf{a}_{pM+m} = \mathbf{u}_m$, where $p = 0, 1, \cdots, P-1$ and $\mathbf{u}_m$ is the m-th column vector of $\mathbf{U}_M$. Thus, we have $\mathbf{u}_m^H \cdot \mathbf{u}_{m'} = M \cdot \delta(m - m')$. Consequently, we can write

$$\mathbf{a}_{pM+m}^H \cdot \mathbf{a}_{p'M+m'} = \mathbf{u}_m^H \cdot \mathbf{u}_{m'} = M \cdot \delta(m - m'). \tag{19}$$

According to (18), the μ-th column of the matrix $\boldsymbol{\mathcal{G}}(z)$ is given by

$$\mathbf{g}_\mu(z) = \Big[g_{0\mu}(z), \ g_{1\mu}(z), \ \cdots, \ g_{(M-1)\mu}(z)\Big]^T, \tag{20}$$

where $0 \leq \mu \leq K-1$ and the sequence $g_{m\mu}(z)$ of length K can be written by

$$g_{m\mu}(z) = \sum_{k=0}^{K-1} a_{mk} \cdot h_{k\mu} \cdot z^{-k}, \tag{21}$$

where $m = 0, 1, \cdots, M-1$. Thus, (21) implies that $g_{m\mu}(z)$ are unimodular sequences of length K. The sum of ACCFs between the μ-th and ν-th columns of the matrix $\boldsymbol{\mathcal{G}}(z)$ is given by

$$\begin{aligned}
S_{\mathbf{g}_\mu, \mathbf{g}_\nu}(z) &= \sum_{m=0}^{M-1} R_{\boldsymbol{g}_{m\mu}, \boldsymbol{g}_{m\nu}}(z) \\
&= \sum_{m=0}^{M-1} \sum_{k=0}^{K-1} \sum_{k'=0}^{K-1} a_{mk} \cdot a_{mk'}^* \cdot h_{k\mu} \cdot h_{k'\nu}^* \cdot z^{-(k'-k)} \\
&= \sum_{\tau=0}^{K-1} \sum_{k=0}^{K-\tau-1} \sum_{m=0}^{M-1} a_{mk} \cdot a_{m(k+\tau)}^* \cdot h_{k\mu} \cdot h_{(k+\tau)\nu}^* \cdot z^{-\tau} \\
&= \sum_{\tau=0}^{M-1} \sum_{k=0}^{K-\tau-1} \mathbf{a}_{k+\tau}^H \cdot \mathbf{a}_k \cdot h_{k\mu} \cdot h_{(k+\tau)\nu}^* \cdot z^{-\tau} \\
&\quad + \sum_{\tau=M}^{K-1} \sum_{k=0}^{K-\tau-1} \sum_{m=0}^{M-1} a_{mk} \cdot a_{m(k+\tau)}^* \cdot h_{k\mu} \cdot h_{(k+\tau)\nu}^* \cdot z^{-\tau} \\
&= \sum_{k=0}^{K-1} \mathbf{a}_k^H \cdot \mathbf{a}_k \cdot h_{k\mu} \cdot h_{k\nu}^* \\
&\quad + \sum_{\tau=M}^{K-1} \sum_{k=0}^{K-\tau-1} \sum_{m=0}^{M-1} a_{mk} \cdot a_{m(k+\tau)}^* \cdot h_{k\mu} \cdot h_{(k+\tau)\nu}^* \cdot z^{-\tau} \\
&= M \sum_{k=0}^{K-1} h_{k\mu} \cdot h_{k\nu}^* \\
&\quad + \sum_{\tau=M}^{K-1} \sum_{k=0}^{K-\tau-1} \sum_{m=0}^{M-1} a_{mk} \cdot a_{m(k+\tau)}^* \cdot h_{k\mu} \cdot h_{(k+\tau)\nu}^* \cdot z^{-\tau} \\
&= MK \cdot \delta(\mu - \nu) \\
&\quad + \sum_{\tau=M}^{K-1} \sum_{k=0}^{K-\tau-1} \sum_{m=0}^{M-1} a_{mk} \cdot a_{m(k+\tau)}^* \cdot h_{k\mu} \cdot h_{(k+\tau)\nu}^* \cdot z^{-\tau}.
\end{aligned}$$

Thus, the matrix of ACCF sums is given by

$$\widetilde{\boldsymbol{\mathcal{G}}(z)} \cdot \boldsymbol{\mathcal{G}}(z) = MK \cdot \mathbf{I}_K \text{ within the ZCZ width } M.$$

That is, $\boldsymbol{\mathcal{G}}(z)$ is a ZPU matrix of size $M \times K$, sequence length K and ZCZ width $Z = M$. Now, $K/M = MP/M = P = \lfloor L/Z \rfloor$. So, $\boldsymbol{\mathcal{G}}(z)$ is an optimal M-PU matrix. This completes the proof. ■

***Remark** 5:* The number of phases of the constructed sequences is $LCM(q_0, q_1)$, where $\mathbf{U}_K = BH(K, q_0)$ and $\mathbf{U}_M = BH(M, q_1)$ with $2 \leq q_0 \leq K$ and $2 \leq q_1 \leq M$.

We illustrate our proposed construction of optimal ZPU matrices by the following example. We give a new 3-PU matrix of size 3×6 and sequence length 6 with 3-phase-shift keying (PSK) constellation as opposed to the case when we will use DFT matrix where the generated sequences belong to the 6-PSK constellation.

***Example** 3:* Let $M = 3$ and $K = 6$ with $P = 2$. Let $\mathbf{U}_K = \mathbf{S}_6 = BH(6, 3)$ given by [12, eq.(19)]. Let $\mathbf{U}_M = \mathbf{F}_3$ and $\mathbf{G} = \Big[\mathbf{F}_3 \quad \mathbf{F}_3\Big]$. Clearly, $\mathbf{G}$ is a 3×6 matrix with 3-PSK constellation. Note that $LCM\,(q_0, q_1) = 3$ with $q_0 = q_1 = 3$. According to our proposed construction method, a 3-PU matrix of size 3×6 and sequence length 6 is given by

$$\boldsymbol{\mathcal{G}}(z) = \mathbf{G} \cdot \mathbf{D}_K(z) \cdot \mathbf{U}_K = \mathbf{G} \cdot \mathbf{D}_6(z) \cdot \mathbf{S}_6, \tag{22}$$

where $\mathbf{D}_6(z) = \text{diag}\Big(1, z^{-1}, z^{-2}, z^{-3}, z^{-4}, z^{-5}\Big)$. The matrix of ACCF sums is given by

$$\widetilde{\boldsymbol{\mathcal{G}}(z)} \cdot \boldsymbol{\mathcal{G}}(z) = 18 \cdot \mathbf{I}_6 \text{ within the ZCZ width } 3. \tag{23}$$

Also, we have $K/M = P = \lfloor L/Z \rfloor$ and hence $\boldsymbol{\mathcal{G}}(z)$ is an optimal 3-PU matrix of size 3×6 and sequence length 6 with 3-PSK constellation. We have written out this 3-PU matrix by Table I in which only the exponents of $\omega = e^{-2\pi\sqrt{-1}/3}$ are given.

Table I: A 3×6 Optimal 3-PU Matrix with Sequence Length 6

$\mathbf{x}_0$	000000 012012 021021	$\mathbf{x}_1$	001122 010101 022110	$\mathbf{x}_2$	010221 022200 001212	$\mathbf{x}_3$	012012 021021 000000	$\mathbf{x}_4$	022101 001110 010122	$\mathbf{x}_5$	021210 000222 012201

According to *Theorem 1*, we have the following corollary for the construction of binary sequences.

***Corollary** 2:* Let $\mathbf{H}_{2^{m+k}}$ and $\mathbf{H}_{2^m}$ be two binary Hadamard matrices of size $2^{m+k} \times 2^{m+k}$ and $2^m \times 2^m$, respectively. Let us consider a block matrix $\mathbf{G} = \Big[\mathbf{H}_{2^m}\ \mathbf{H}_{2^m}\ \cdots\ \mathbf{H}_{2^m}\ (2^k \text{ times})\Big]$ with size $2^m \times 2^{m+k}$. Then, the matrix $\mathcal{G}(z)$ given by (18) is an optimal binary 2^m-PU matrix of size $2^m \times 2^{m+k}$ and sequence length 2^{m+k}.

B. Comparison with Previous Works on ZCCSs

In the literature, there are main three types of construction methods for ZCCSs. The first type is based on seed Z-complementary sequence pairs [19], [22]. The second type is based on complementary sequence pairs [20], [21], [24]. The third type is the direct construction methods based on generalized Boolean functions [25], [26]. According to this classification, we can see that most algorithms have been concerned with ZCCSs when the number of constituent sequences is restricted to two. [25], and [26] studied ZCCSs when the number of constituent sequences can be more than two. However, the constructed ZCCS parameters for their construction methods are all limited to powers of two. Our proposed construction framework offers more flexibilities on the ZCCSs parameters compared to the previously known works. For example, an optimal $(6, 3)$-ZCCS$_3^6$ with 3-PSK constellation given by Table I may not be obtained by the previously known methods.

V. CONCLUSION AND FUTURE WORK

In this paper, we have investigated a new concept of ZPU matrices. It is shown that there exists an equivalence between a ZPU matrix and ZCCS. Thus, the proposed ZPU matrices have neither limitation on the sequence lengths nor limitation on the matrix sizes. In addition, we have investigated a simple construction of optimal ZPU matrices based on BH matrices. The proposed construction method offers more choices in ZCCS parameters compared to the previous works.

ACKNOWLEDGMENT

S. Das is a visiting Ph.D. student with The University of Melbourne, Melbourne 3010, Australia, on academic leave from the Department of Mathematics, IIT Patna, India 801103. The works of S. Das and U. Parampalli are supported in part by the "Communications Sensing and Coding (CSI-CSC) Research Network", of the University of Melbourne. The work of S. Majhi was supported in part by the Visvesvaraya Young Faculty Research Fellowship, Ministry of Electronics and Information Technology, Government of India, being implemented by the Digital India Corporation. S. Das would like to thank Dr. Srdjan Budišin at the RT-RK, Novi Sad, Serbia for the insightful discussions.

REFERENCES

[1] T. Kailath, *Linear systems*. Prentice-Hall Englewood Cliffs, NJ, 1980, vol. 156.

[2] P. P. Vaidyanathan, *Multi-rate systems and filter banks*. Prentice Hall, 1993.

[3] S. Z. Budišin and P. Spasojević, "Paraunitary generation/correlation of QAM complementary sequence pairs," in *Proc. Cryptography and Communications 6.1*, Oct. 2014, pp. 59–102.

[4] E. Kofidis and P. A. Regalia, "Spreading sequence design via perfect-reconstruction filter banks," *CiteSeerX*, 2014.

[5] S. M. Phoong and P. P. Vaidyanathan, "Paraunitary filter banks over finite fields," *IEEE Trans. Signal Process.*, vol. 45, no. 6, pp. 1443–1457, Jun. 1997.

[6] S. M. Phoong and K.-Y. Chang, "Antipodal paraunitary matrices and their application to OFDM systems," *IEEE Trans. Signal Process.*, vol. 53, no. 4, pp. 1374–1386, Apr. 2005.

[7] G. W. Wornell, "Spread-signature CDMA: efficient multiuser communication in the presence of fading," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1418–1438, Sep. 1995.

[8] F. Delgosha and F. Fekri, "Public-key cryptography using paraunitary matrices," *IEEE Trans. Signal Process.*, vol. 54, no. 9, pp. 3489–3504, Sep. 2006.

[9] Y. C. Jen, S. M. Phoong, Y. H. Chung, and H. J. Su, "Method of handling antipodal parauitary precoding for MIMO-OFDM and related communication device," Oct. 2012, US Patent App. 13/271,258. [Online]. Available: https://www.google.com/patents/US20120269284

[10] Z. Wang, G. Wu, and D. Ma, "A new method to construct Golay complementary set by paraunitary matrices and Hadamard matrices," in *Proc. 9th International Conference on Sequences and Their Applications (SETA-2016)*, Sep. 2016, pp. 1–12.

[11] S. Das, S. Majhi, S. Budišin, Z. Liu, and Y. L. Guan, "A novel multiplier-free generator for complete complementary codes," in *Proc. 23rd Asia-Pacific Conference on Communications (APCC)*, Dec. 2017.

[12] S. Das, S. Budišin, S. Majhi, Z. Liu, and Y. L. Guan, "A multiplier-free generator for polyphase complete complementary codes," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1184–1196, Nov. 2017.

[13] S. Z. Budišin and P. Spasojević, "Paraunitary-based Boolean generator for QAM complementary sequences of length 2^K," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5938–5956, Aug. 2018.

[14] S. Das, S. Majhi, and P. Sarkar, "An improved multiplier-free generator for polyphase complete complementary codes," in *Proc. 10th International Conference on Sequences and Their Applications (SETA-2018)*, Oct. 2018, pp. 1–12.

[15] D. Ma, S. Budišin, Z. Wang, and G. Gong, "A new generalized paraunitary generator for complementary sets and complete complementary codes of size 2^m," *IEEE Signal Process. Lett.*, vol. 26, no. 1, pp. 4–8, Oct. 2018.

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

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

[18] S. Das, U. Parampalli, S. Majhi, and Z. Liu, "Near-optimal zero correlation zone sequence sets from paraunitary matrices," in *Proc. IEEE Int. Sym. Inf. Theory (ISIT-2019), Accepted*, Jul. 2019, pp. 1–5.

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

[20] Z. Liu, U. Parampalli, and Y. L. Guan, "On even-period binary Z-complementary pairs with large ZCZs," *IEEE Signal Process. Lett.*, vol. 21, no. 3, pp. 284–287, Mar. 2014.

[21] ——, "Optimal odd-length binary Z-complementary pairs," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5768–5781, Sep. 2014.

[22] X. Li, W. H. Mow, and X. Niu, "New construction of Z-complementary pairs," *Electron. Lett.*, vol. 52, no. 8, pp. 609–611, 2016.

[23] A. R. Adhikary, Z. Liu, Y. L. Guan, S. Majhi, and S. Z. Budishin, "Optimal binary periodic almost-complementary pairs," *IEEE Signal Process. Lett.*, vol. 23, no. 12, pp. 1816–1820, Dec. 2016.

[24] A. R. Adhikary, S. Majhi, Z. Liu, and Y. L. Guan, "New sets of even-length binary Z-complementary pairs with asymptotic ZCZ ratio of $3/4$," *IEEE Signal Process. Lett.*, vol. 25, no. 7, pp. 970–973, Jul. 2018.

[25] S. Wu and C. Chen, "Optimal Z-complementary sequence sets with good peak-to-average power-ratio property," *IEEE Signal Process. Lett.*, vol. 25, no. 10, pp. 1500–1504, Oct. 2018.

[26] P. Sarkar, S. Majhi, and Z. Liu, "Optimal Z-complementary code set from generalized Reed-Muller codes," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 1783–1796, Mar. 2019.

[27] P. Sarkar, S. Majhi, H. Vettikalladi, and A. S. Mahajumi, "A direct construction of inter-group complementary code set," *IEEE Access*, vol. 6, pp. 42 047–42 056, Aug. 2018.

[28] A. T. Butson, "Generalized Hadamard matrices," in *Proc. Am. Math. Soc. 13*, 1962, pp. 894–898.

[29] Z. Liu, Y. L. Guan, B. C. Ng, and H. Chen, "Correlation and set size bounds of complementary sequences with low correlation zone," *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3285–3289, Dec. 2011.