A Novel Multiplier-Free Generator for Complete Complementary Codes

S. Das and S. Majhi
Department of Mathematics
Indian Institute of Technology Patna
Patna, India 801106
Email:{shibsankar.pma15, smajhi}@iitp.ac.in

S. Budišin
RT-RK, Novi Sad
Serbia, 21000
Email: budishin@gmail.com

Z. Liu and Y. L. Guan
School of EEE
Nanyang Technological University
Singapore 639798
Email:{zilongliu, eylguan}@ntu.edu.sg

***Abstract*—Owing to their ideal correlation properties, complete complementary codes (CCC) have found numerous applications in wireless engineering, in particular they have been employed to support interference-free multi-carrier code-division multiple access systems with improved spectral efficiency. In this paper, we propose a simple construction of CCCs of length N^n ($n \in \mathbb{N}$) based on paraunitary matrices of size $N \times N$. This algorithm can generate CCCs from N-shift cross-orthogonal sequence sets for $n > 1$. Then, we introduce an easy implementation of the proposed algorithm by multiplexers and read-only memories (ROMs), i.e., a multiplier-free implementation. As multipliers are avoided, substantial reduction of construction complexity for CCCs is obtained as compared to the existing works.**

I. Introduction

Complementary sets of sequences (CSS) have been long studied for their vast number of applications in multi-emission systems [1] and multi-carrier CDMA (MC-CDMA) systems [2], [3]. They have also been successfully employed in the construction of zero correlation zone (ZCZ) sequences [4]- [6] and generalized pairwise complementary sequences [7].

In 1972, Tseng and Liu extended the concept of complementary sequences to mutually orthogonal complementary code set (MOCCS) [8], in which every pair of complementary codes have zero aperiodic cross-correlation function (ACCF) sums for all time-shifts. Later, Suehiro and Hatori proposed N-shift cross-orthogonal sequence sets (N-CO-SSs) and extended the idea of MOCCS to complete complementary codes (CCC) in [9]. They constructed CCCs from the N-CO-SSs. These type of CCCs are called N-shift cross-orthogonal CCCs (N-CO-CCCs). However, the algorithm given in [9] has a limitation that the length of the sequences in the generated CCC must be not smaller than N^2 which degrades the spectral efficiency of CCC based CDMA systems [10], [11]. To overcome this limitation, many improved algorithms [12]- [14] have been proposed for the construction of CCCs. There are also other algorithms for CCCs such as, from existing CCC [15], from Reed-Muller codes [16], from generalized Boolean functions [17] etc.

In recent years, the applications of CCC have been extended to MC-CDMA systems for their ideal correlation properties. Non-ideal correlation properties of spreading sequences results in multi-path interference (MPI) and multi-user interference (MUI) which degrades the system performance. The ideal correlation properties of CCC yields interference-free performance for an asynchronous uplink CDMA system [18].

Nowadays, an extremely important task in the study of CSS is to reduce the construction complexity. In this paper, we first propose a new generator for CCCs of length N^n ($n \in \mathbb{N}$) based on paraunitary (PU) matrices of size $N \times N$. We show that the proposed algorithm can generate N-CO-CCCs of length N^n ($n > 1$). Then we propose an easy implementation of our proposed algorithm for CSS by using multiplexers and read-only memories (ROMs). This allows us to generate CCCs without using multipliers. That is, we find a way to avoid multipliers in the construction of CCCs. As multipliers are avoided, substantial reduction of construction complexity for CCCs is obtained as compared to the existing works [9], [12]- [14]. Therefore, the CCCs constructed by the proposed algorithm may be used in interference-free MC-CDMA system with low implementation cost.

The remainder of this work is organized as follows, Section II presents some basic definitions, notations and preliminaries. In Section III, a simple construction of CCCs has been developed. An easy implementation of our proposed algorithm without multipliers is presented in Section IV. Finally, we summarize our works in Section V.

II. Preliminaries

This section presents some basic definitions, notations and preliminaries.

A. ACCF and AACF

Given two length-L complex-valued sequences $\boldsymbol{x} = [x[0], x[1], \cdots, x[L-1]]$ and $\boldsymbol{y} = [y[0], y[1], \cdots, y[L-1]]$, their aperiodic correlation function at time-shift τ is defined as

$$R_{\boldsymbol{x},\boldsymbol{y}}[\tau] = \begin{cases} \sum_{k=0}^{L-1-\tau} x[k]y^*[k+\tau], & 0 \leqslant \tau \leqslant L-1 \\ \sum_{k=0}^{L-1+\tau} x[k-\tau]y^*[k], & 1-L \leqslant \tau < 0 \\ 0, & \text{otherwise,} \end{cases} \tag{1}$$

where $y^*[k]$ denotes the complex conjugate of $y[k]$.

The above is called aperiodic cross-correlation function (ACCF) when $\boldsymbol{x} \neq \boldsymbol{y}$; Otherwise, it is called aperiodic auto-correlation function (AACF). For simplicity, the AACF of $\boldsymbol{x}$ will be written as $R_{\boldsymbol{x}}[\tau]$.

The Z-transform of a sequence $\boldsymbol{x}$ is defined by

$$x(Z^{-1}) = \sum_{k=0}^{L-1} x[k]Z^{-k}. \tag{2}$$

We use the convention that its complex conjugate is

$$x^*(Z^{-1}) = \sum_{k=0}^{L-1} x^*[k]Z^{-k}. \tag{3}$$

A reverted sequence is a sequence whose elements are inverted in time as $x^R[k] = x[L-1-k]$. Its Z-transform is $x^R(Z^{-1}) = Z^{-L+1}x(Z)$.

The Z-transform of the ACCF $R_{\boldsymbol{x},\boldsymbol{y}}[\tau]$ between $\boldsymbol{x}$ and $\boldsymbol{y}$ is given by

$$R_{\boldsymbol{x},\boldsymbol{y}}(Z^{-1}) = \sum_{k=0}^{L-1} R_{\boldsymbol{x},\boldsymbol{y}}[k]Z^{-k} = x(Z)y^*(Z^{-1}). \tag{4}$$

The Z-transform of the AACF $R_{\boldsymbol{x}}[k]$ is given by

$$R_{\boldsymbol{x}}(Z^{-1}) = \sum_{k=0}^{L-1} R_{\boldsymbol{x}}[k]Z^{-k} = x(Z)x^*(Z^{-1}). \tag{5}$$

B. N-shift Cross-orthogonal Sequence Sets (N-CO-SSs)

Definition 1 (N-AO-S [9]): An N-shift auto-orthogonal sequence (N-AO-S) of length L is defined as a sequence $\boldsymbol{x}$ whose AACF $R_{\boldsymbol{x}}[\tau]$ is 0 for any N-multiple shift except the zero shift:

$$R_{\boldsymbol{x}}[\tau] = 0 \quad \text{for } \tau = \pm N, \pm 2N, \cdots. \tag{6}$$

Definition 2 (N-CO-S [9]): A pair of N-shift cross-orthogonal sequences (N-CO-Ss) of length L is defined as a pair of sequences $\boldsymbol{x}$ and $\boldsymbol{y}$ both of length L whose ACCF $R_{\boldsymbol{x},\boldsymbol{y}}[\tau]$ is 0 for any N-multiple shift (including the zero-shift):

$$R_{\boldsymbol{x},\boldsymbol{y}}[\tau] = 0 \quad \text{for } \tau = 0, \pm N, \pm 2N, \cdots. \tag{7}$$

Definition 3 (N-CO-SS [9]): A set of M sequences $\{\boldsymbol{x}^{(0)}, \boldsymbol{x}^{(1)}, \cdots, \boldsymbol{x}^{(M-1)}\}$ is called N-shift cross-orthogonal sequence set (N-CO-SS) when any two out of the M sequences form a pair of N-CO-Ss.

C. Complementary Set of Sequences (CSS)

Definition 4 (CSP [19]): A pair of sequences $(\boldsymbol{x}, \boldsymbol{y})$ is said to be a complementary sequence pair (CSP) if $R_{\boldsymbol{x}}(Z^{-1}) + R_{\boldsymbol{y}}(Z^{-1}) = c$, where c is a positive constant.

Definition 5 (CSS [19]): A set $\{\boldsymbol{x}^{(0)}, \boldsymbol{x}^{(1)}, \cdots, \boldsymbol{x}^{(M-1)}\}$ of M equally long sequences is said to be a CSS if

$$\sum_{m=0}^{M-1} R_{\boldsymbol{x}^{(m)}}(Z^{-1}) = \sum_{m=0}^{M-1} x^{(m)}(Z)x^{(m)*}(Z^{-1}) = c. \tag{8}$$

D. Complete Complementary Codes (CCC)

Let $\mathcal{C} = \{\mathbf{x}_0(Z^{-1}), \mathbf{x}_1(Z^{-1}), \cdots, \mathbf{x}_{K-1}(Z^{-1})\}$ be a set of K column vectors, each of size M, i.e.,

$$\mathbf{x}_\mu(Z^{-1}) = \left[x_\mu^{(0)}(Z^{-1}), \cdots, x_\mu^{(M-1)}(Z^{-1})\right]^T, \tag{9}$$

where $0 \leqslant \mu \leqslant K-1$ and $x_\mu^{(m)}(Z^{-1})$ is a sequence, $m \in \{0, 1, \cdots, M-1\}$.

The Z-transform of the sum of ACCFs between $\mathbf{x}_\mu(Z^{-1})$ and $\mathbf{x}_\nu(Z^{-1})$ (where $0 \leqslant \mu, \nu \leqslant K-1$) is defined as

$$S_{\mathbf{x}_\mu,\mathbf{x}_\nu}(Z^{-1}) = \sum_{m=0}^{M-1} R_{\boldsymbol{x}_\mu^{(m)},\boldsymbol{x}_\nu^{(m)}}(Z^{-1}) = \widetilde{\mathbf{x}_\nu(Z)}\mathbf{x}_\mu(Z), \tag{10}$$

where the tilde operator is defined as $\widetilde{\mathbf{x}_\nu(Z^{-1})} = \mathbf{x}_\nu^H(Z)$, H is Hermitian operation.

Definition 6 (MOCCS [17]): $\mathcal{C}$ is said to be a (K, M, L)-mutually orthogonal complementary code set (MOCCS) [8] if

$$\widetilde{\mathbf{x}_\nu(Z)}\mathbf{x}_\mu(Z) = c\delta(\mu - \nu), \tag{11}$$

where δ is Kronecker delta function. It has been proven that $K \leqslant M$ [20], [21], where K and M denote set size of MOCCS and the number of constituent sequences respectively. When $K = M$, $\mathcal{C}$ is said to be a set of CCC [9].

We call a set of CCC generated from N-CO-SS as N-shift cross-orthogonal CCC (N-CO-CCC) throughout this paper.

E. M-ary Representation

Definition 7: The M-ary representation of a non-negative number k with r digits is defined by

$$k = \sum_{m=0}^{r-1} k_m M^m; \quad k_m \in \{0, 1, \cdots, M-1\} \tag{12}$$

In the M-ary representation of k, k_m are said to be digits. The string of digits $k_{r-1}k_{r-2}\cdots k_0$ denotes the number k.

F. Paraunitary (PU) Matrices

PU matrices are simply matrices of polynomials over Z^{-1} that are unitary for any $|Z| = 1$. So PU matrices are the generalization of unitary matrices. A polynomial matrix of size $p \times q$ is defined as $\mathbf{X}(Z^{-1}) = \left[x_{lm}(Z^{-1})\right]; \quad 0 \leqslant l \leqslant p-1, 0 \leqslant m \leqslant q-1$.

In general, the definition of PU matrices is also valid for non-square matrices. We can define a wide sense PU matrix of size $p \times q$ using tilde operator by the relation

$$\widetilde{\mathbf{X}(Z^{-1})}\mathbf{X}(Z^{-1}) = c\mathbf{I}_q, \tag{13}$$

where $\mathbf{I}_q$ is an identity matrix of size $q \times q$ and tilde operator is defined by

$$\widetilde{\mathbf{X}(Z^{-1})} = \mathbf{X}^H(Z). \tag{14}$$

We denote by $\mathbf{x}(Z^{-1})$ a PU column vector.

Next, an important connection between PU matrices and CSS is given by the following theorem.

Theorem 1: A column vector consisting of Z-transforms of M sequences is a CSS iff it is a PU column vector of size M.

Proof: Let $\mathbf{x}(Z^{-1}) = \left[x^{(0)}(Z^{-1}), x^{(1)}(Z^{-1}), \cdots, x^{(M-1)}(Z^{-1})\right]^T$ be a column vector consisting of Z-transforms of M sequences of equal length. According to (13), $\widetilde{\mathbf{x}(Z^{-1})}\mathbf{x}(Z^{-1}) = c$ iff $\sum_{m=0}^{M-1} R_{\boldsymbol{x}^{(m)}}(Z^{-1}) = c$ which is the same as (8). ■

Remark 1: The above *Theorem 1* shows that there is an equivalence between PU matrices and CSS. This equivalence allows us to apply the concept of PU matrices from the theory of filter-banks [22] to the field of complementary sequence design.

Definition 8: As any PU column vector of degree $L-1$ can be expressed as a product of a square PU matrix $\boldsymbol{\mathcal{G}}(Z^{-1})$ of degree $L-1$ and a constant column vector $\mathbf{v}$ [22], we have

$$\mathbf{x}(Z^{-1}) = \boldsymbol{\mathcal{G}}\left(Z^{-1}\right)\mathbf{v}. \tag{15}$$

We define $\boldsymbol{\mathcal{G}}(Z^{-1})$ as generating matrix for the sequence set $\mathbf{x}(Z^{-1})$ of length L. Note that (15) is not a unique representation.

III. The Proposed Algorithm for Complete Complementary Codes

In this section, we propose a recursive construction of CCCs on the basis of PU matrices.

A. Proposed PU Construction for CCC

Let $\mathbf{U}_n = \left[u_{lm}^{(n)}\right]$ be a unitary matrix of size $N \times N$ such that $\left|u_{lm}^{(n)}\right| = 1$. Our proposed recursive construction is given by

$$\boldsymbol{\mathcal{G}}_n\left(Z^{-1}\right) = \boldsymbol{\mathcal{G}}_{n-1}\left(Z^{-N}\right)\mathbf{D}_1\left(Z^{-1}\right)\mathbf{U}_n, \tag{16}$$

where $\boldsymbol{\mathcal{G}}_0(Z^{-1}) = \mathbf{U}_0$, $n \in \mathbb{N}$ and $\mathbf{D}_1\left(Z^{-1}\right)$ is defined by

$$\mathbf{D}_1(Z^{-1}) = \text{diag}\left(1, Z^{-1}, \cdots, Z^{-(N-1)}\right). \tag{17}$$

Remark 2: Let m and k be two positive integers. If we define $\mathbf{D}_m(Z^{-1}) = \text{diag}\left(1, Z^{-m}, \cdots, Z^{-(N-1)m}\right)$, then $\mathbf{D}_m(Z^{-k}) = \text{diag}\left(1, Z^{-mk}, \cdots, Z^{-(N-1)mk}\right) = \mathbf{D}_{mk}(Z^{-1})$.

Using *Remark 2*, the expanded form of the PU product from (16) is given by

$$\boldsymbol{\mathcal{G}}_n(Z^{-1}) = \left\{\prod_{r=n}^{1}(\mathbf{U}_{n-r}\mathbf{D}_{N^{r-1}}(Z^{-1}))\right\}\mathbf{U}_n. \tag{18}$$

By the property of PU matrix, we can say that $\boldsymbol{\mathcal{G}}_n(Z^{-1})$ is PU matrix for each $n \in \mathbb{N}$. Thus, the PU generator for sets is given by

$$\mathbf{x}_{n,j}(Z^{-1}) = \boldsymbol{\mathcal{G}}_n(Z^{-1})\mathbf{e}_j^T, \tag{19}$$

where $\mathbf{e}_j$ is the jth row vector of $\mathbf{I}_N$, $j = 0, 1, \cdots, N-1$. According to (18), (19) can be written in recursive form as follows:

$$\mathbf{x}_{r,j}(Z^{-1}) = \mathbf{U}_{n-r}\mathbf{D}_{N^{r-1}}(Z^{-1})\mathbf{x}_{r-1,j}(Z^{-1}), \tag{20}$$

where $\mathbf{x}_{0,j}(Z^{-1}) = \mathbf{U}_n\mathbf{e}_j^T$ for $r = 1, 2, \cdots, n$.

For the set

$$\mathbf{x}_{r,j}(Z^{-1}) = \left[x_{r,j}^{(0)}(Z^{-1}), \cdots, x_{r,j}^{(N-1)}(Z^{-1})\right]^T \tag{21}$$

generated by (20) in r iteration, the sequences $x_{r,j}^{(l)}(Z^{-1})$ can be expressed as follows:

$$\begin{aligned} &x_{r,j}^{(l)}(Z^{-1}) \\ &= u_{l0}^{(n-r)}x_{r-1,j}^{(0)}(Z^{-1}) + u_{l1}^{(n-r)}x_{r-1,j}^{(1)}(Z^{-1})Z^{-N^{r-1}} \\ &\quad + \cdots + u_{lN-1}^{(n-r)}x_{r-1,j}^{(N-1)}(Z^{-1})Z^{-(N-1)N^{r-1}}, \end{aligned} \tag{22}$$

where $l = 0, 1, \cdots, N-1$. Since the values of the sequence $x_{r-1,j}^{(l)}[k]$ outside the range $0 \le k \le N^{r-1}-1$ will be zero, the above (22) can be written in time-domain as follows:

$$x_{r,j}^{(l)}[k] = u_{lk_{r-1}}^{(n-r)}x_{r-1,j}^{(k_{r-1})}\left[k - k_{r-1}N^{r-1}\right], \tag{23}$$

where k has digits $k_0, k_1, \cdots, k_{r-1}$ in the N-ary expansion given by (12).

In order to illustrate the time-domain expression (23) derived from (22), one example is given.

Example 1: Let $N = 2$ and $n = 3$. Let us consider the set $\mathbf{x}_{3,j}(Z^{-1}) = \left[x_{3,j}^{(0)}(Z^{-1}), x_{3,j}^{(1)}(Z^{-1})\right]^T$ generated by (20) in $r = 3$ iteration. Therefore, the sequences $x_{3,j}^{(0)}(Z^{-1})$ and $x_{3,j}^{(1)}(Z^{-1})$ can be written by

$$x_{3,j}^{(l)}(Z^{-1}) = u_{l0}^{(1)}x_{2,j}^{(0)}(Z^{-1}) + u_{l1}^{(1)}x_{2,j}^{(1)}(Z^{-1})Z^{-2^2}, \tag{24}$$

where $l = 0, 1$. The sequences $x_{2,j}^{(0)}(Z^{-1})$ and $x_{2,j}^{(1)}(Z^{-1})$ have length 2^2. By using the definition of Z-transform (given by (2)), then (24) can be expressed as:

$$\begin{aligned} &x_{3,j}^{(l)}(Z^{-1}) \\ &= u_{l0}^{(1)}\Big(x_{2,j}^{(0)}[0] + x_{2,j}^{(0)}[1]Z^{-1} + x_{2,j}^{(0)}[2]Z^{-2} + x_{2,j}^{(0)}[3] \\ &\quad Z^{-3}\Big) + u_{l1}^{(1)}\Big(x_{2,j}^{(1)}\left[4-2^2\right]Z^{-4} + x_{2,j}^{(1)}\left[5-2^2\right]Z^{-5} \\ &\quad + x_{2,j}^{(1)}\left[6-2^2\right]Z^{-6} + x_{2,j}^{(1)}\left[7-2^2\right]Z^{-7}\Big). \end{aligned} \tag{25}$$

Thus, the sequence $x_{3,j}^{(l)}(Z^{-1})$ (having length 2^3) can be expressed in time-domain as follows:

$$x_{3,j}^{(l)}[k] = u_{lk_2}^{(1)}x_{2,j}^{(k_2)}\left[k - k_2 2^2\right], \tag{26}$$

where k has binary digits k_0, k_1 and k_2.

We are now ready to prove the following proposition.

Proposition 1: The set $\boldsymbol{\mathcal{G}}_n(Z^{-1})$ generated by the algorithm (16) is CCC of length N^n for $n \in \mathbb{N}$.

Proof: Let i and j be two integers from the set $\{0, 1, \cdots, N-1\}$. For the two sequence sets $\mathbf{x}_{n,i}(Z^{-1}) = \boldsymbol{\mathcal{G}}_n(Z^{-1})\mathbf{e}_i^T$ and $\mathbf{x}_{n,j}(Z^{-1}) = \boldsymbol{\mathcal{G}}_n(Z^{-1})\mathbf{e}_j^T$, we have

$$\begin{aligned} S_{\mathbf{x}_{n,i},\mathbf{x}_{n,j}}(Z^{-1}) &= \widetilde{\mathbf{x}_{n,j}(Z)}\mathbf{x}_{n,i}(Z) = \widetilde{\boldsymbol{\mathcal{G}}_n(Z)}\mathbf{e}_j^T\boldsymbol{\mathcal{G}}_n(Z)\mathbf{e}_i^T \\ &= \mathbf{e}_j^T\widetilde{\boldsymbol{\mathcal{G}}_n(Z)}\boldsymbol{\mathcal{G}}_n(Z)\mathbf{e}_i^T. \end{aligned} \tag{27}$$

As $\boldsymbol{\mathcal{G}}_n(Z^{-1})$ is a PU matrix, $\widetilde{\boldsymbol{\mathcal{G}}_n(Z^{-1})}\boldsymbol{\mathcal{G}}_n(Z^{-1}) = c\mathbf{I}_N$, thus

$$S_{\mathbf{x}_{n,i},\mathbf{x}_{n,j}}(Z^{-1}) = c\widetilde{\mathbf{e}_j^T}\mathbf{e}_i^T = c\mathbf{e}_j\mathbf{e}_i^T = c\delta(j-i). \tag{28}$$

For $i = j$, we get $S_{\mathbf{x}_{n,i},\mathbf{x}_{n,i}}(Z^{-1}) = c$ which means that the corresponding set is a CSS. For $i \neq j$ we get, $S_{\mathbf{x}_{n,i},\mathbf{x}_{n,j}}(Z^{-1}) = 0$ which means that both sets are mutually orthogonal. Since i and j are chosen arbitrarily from the set $\{0, 1, \cdots, N-1\}$, they form a set of CCC. ∎

Remark 3: We have seen that each column of $\boldsymbol{\mathcal{G}}_n(Z^{-1})$ is CSS and different columns are mutually orthogonal. It can similarly be shown that each row of $\boldsymbol{\mathcal{G}}_n(Z^{-1})$ is CSS and different rows are mutually orthogonal.

We give an example of the construction of CCC.

Example 2: Let $N = 3$ and $n = 3$. Let us consider the DFT matrix $\mathbf{F}_3 = \left[\omega^{lm}\right]$ ($\omega = e^{-2\pi\sqrt{-1}/3}$) of size

3×3 as unitary matrix. According to (16), we obtain CCC, $\mathcal{C} = \{\mathbf{x}_{3,0}, \mathbf{x}_{3,1}, \mathbf{x}_{3,2}\}$ shown in TABLE I where only exponents of ω are given.

TABLE I
$\mathcal{C} = \{\mathbf{x}_{3,0}, \mathbf{x}_{3,1}, \mathbf{x}_{3,2}\}$ OF LENGTH 3^3.

$\mathbf{x}_{3,0}$	000012021000120210000201102
	000012021111201021222120021
	000012021222012102111012210
$\mathbf{x}_{3,1}$	012021000012102222012210111
	012021000120210000201102000
	012021000201021111120021222
$\mathbf{x}_{3,2}$	021000012021111201021222120
	021000012102222012210111012
	021000012210000120102000201

Next, we show that the proposed algorithm (16) generates N-CO-CCCs for $n > 1$. For that our first step is to prove the following proposition.

Proposition 2: The sequence set $\mathbf{y}_n(Z^{-1}) = \boldsymbol{\mathcal{G}}_{n-1}(Z^{-N}) \left[1, Z^{-1}, \cdots, Z^{-(N-1)}\right]^T$ is N-CO-SS of length N^n ($n > 1$), where $\boldsymbol{\mathcal{G}}_{n-1}(Z^{-1})$ is generated by the algorithm (16).

Proof: Let $\mathbf{y}_n(Z^{-1}) = \Big[y_0(Z^{-1}),\ y_1(Z^{-1}),\ \cdots,\ y_{N-1}(Z^{-1})\Big]^T$ and $\boldsymbol{\mathcal{G}}_{n-1}(Z^{-1}) = \left[g_{ij}(Z^{-1})\right]_{N\times N}$ be a set of CCC of length N^{n-1}. Then we have

$$\begin{aligned} y_i(Z^{-1}) =& g_{i0}(Z^{-N}) + g_{i1}(Z^{-N})Z^{-1} + \\ & \cdots + g_{i(N-1)}(Z^{-N})Z^{-(N-1)} \end{aligned} \tag{29}$$

for $i = 0, 1, \cdots, N-1$. Thus, the sequence $y_i(Z^{-1})$ is generated by interleaving the sequences $g_{i0}(Z^{-1})$, $g_{i1}(Z^{-1}), \cdots, g_{i(N-1)}(Z^{-1})$ which implies that $y_i(Z^{-1})$ has length N^n. Therefore, for any $i, j = 0, 1, \cdots, N-1$, the ACCF $R_{\boldsymbol{y}_i,\boldsymbol{y}_j}[\tau]$ for kN shift is equal to $\frac{1}{N}\sum_{r=0}^{N-1} R_{\boldsymbol{g}_{ir},\boldsymbol{g}_{jr}}[\tau]$ for k shift, where k is an integer. Since $\boldsymbol{\mathcal{G}}_{n-1}(Z^{-1})$ is CCC, $y_i(Z^{-1})$ and $y_j(Z^{-1})$ are N-CO-Ss. As i and j are arbitrary in the set $\{0, 1, \cdots, N-1\}$, the set $[\ y_0(Z^{-1}),\ y_1(Z^{-1}),\ \cdots,\ y_{N-1}(Z^{-1})\ ]^T$ is N-CO-SS of length N^n. ■

To illustrate *Proposition 2*, we give an example below.

Example 3: Let $N = 3$, $n = 3$ and $\boldsymbol{\mathcal{G}}_2(Z^{-1}) = \left[g_{ij}(Z^{-1})\right]_{3\times 3}$, where each $g_{ij}(Z^{-1})$ denotes sequence of length 3^2. The sequences $y_i(Z^{-1})$ ($i = 0, 1, 2$) are given by

$$y_i(Z^{-1}) = g_{i0}(Z^{-3}) + g_{i1}(Z^{-3})Z^{-1} + g_{i2}(Z^{-3})Z^{-2} \tag{30}$$

i.e.,

$$\begin{aligned} \boldsymbol{y}_i =& \Big(g_{i0}[0], g_{i1}[0], g_{i2}[0], g_{i0}[1], g_{i1}[1], g_{i2}[1], \\ & \cdots, g_{i0}[8], g_{i1}[8], g_{i2}[8]\Big). \end{aligned} \tag{31}$$

Therefore, the sequence $y_i(Z^{-1})$ (having length 3^3) is obtained by interleaving the sequences $g_{i0}(Z^{-1}), g_{i1}(Z^{-1})$ and $g_{i2}(Z^{-1})$. Since $\boldsymbol{\mathcal{G}}_2(Z^{-1})$ is CCC, for $i \neq j$ the ACCF $R_{\boldsymbol{y}_i,\boldsymbol{y}_j}[\tau] = 0$ for $\tau = 0, \pm 3, \pm 6, \cdots$. Thus, the sequences $y_0(Z^{-1})$, $y_1(Z^{-1})$ and $y_2(Z^{-1})$ form N-CO-SS of length 3^3.

Based on *Proposition 1* and *Proposition 2*, we are now ready to prove the following proposition.

Proposition 3: The set $\boldsymbol{\mathcal{G}}_n(Z^{-1})$ generated by the algorithm (16) forms N-CO-CCC of length N^n for $n > 1$.

Proof: The proof of this proposition follows directly from the above *Proposition 1* and *Proposition 2*. ■

IV. Multiplier-free Implementation

In this section, we implement our proposed algorithm by using multiplexers and ROMs which results a new generator without multipliers.

A. Implementing the Unitary Transform without Adders

Usually matrix multiplications are performed using scalar multiplications and additions. But we show that no additions are needed for matrix multiplications in (20). According to recursive form (20), in each iteration, the number of non-zero elements is increased by N times compared to previous iteration. In the last iteration, N^n consecutive unimodular elements are generated. So there is no overlapping between any two elements of the sequences. The input vector to the unitary matrix block contains only one non-zero element at any discrete time, so a non-zero element is always added to zero elements and hence these additions can be omitted. Non-zero values at the input to the unitary matrix block are then multiplied by the corresponding elements of the unitary matrix to produce outputs. So the matrix multiplication with the unitary matrix reduces to N scalar multiplications. However, the position of the non-zero signal depends on the discrete time variable k, so we need a multiplexer to select the right signal to be multiplied by the element of unitary matrix.

B. Implementation Based on Multiplexers and ROMs

As no additions are needed in matrix multiplication we can replace the unitary matrix with a multiplexer which chooses the only non-zero input element, a ROM which stores unitary matrix elements and multipliers. The corresponding PU generator is shown in Fig. 1.

According to Fig. 1, we can see that the non-zero signals $x_{r-1,j}^{(l)}[k]$ after the delays at the input of the $\mathbf{U}_{n-r}$ block can be expressed by

$$y_{r-1,j}^{(l)}[k] = x_{r-1,j}^{(l)}\left[k - lN^{r-1}\right], \tag{32}$$

where $k = \sum_{m=0}^{r-2} k_m N^m$. The non-zero output of rth multiplexer with the control (CTRL) signal k_{r-1} can be written by replacing $l = k_{r-1}$ in (32) as follows:

$$y_{r-1,j}^{(k_{r-1})}[k] = x_{r-1,j}^{(k_{r-1})}\left[k - k_{r-1}N^{r-1}\right], \tag{33}$$

where $k = \sum_{m=0}^{r-1} k_m N^m$. Again for the column address k_{r-1}, the ROM outputs are:

$$h_{lk_{r-1}} = u_{lk_{r-1}}^{(n-r)}. \tag{34}$$

Thus, the non-zero outputs of the multipliers are the product of (33) and (34) given by

$$\begin{aligned} x_{r,j}^{(l)}[k] =& h_{lk_{r-1}} y_{r-1,j}^{(k_{r-1})}[k] \\ =& u_{lk_{r-1}}^{(n-r)} x_{r-1,j}^{(k_{r-1})}\left[k - k_{r-1}N^{r-1}\right], \end{aligned} \tag{35}$$

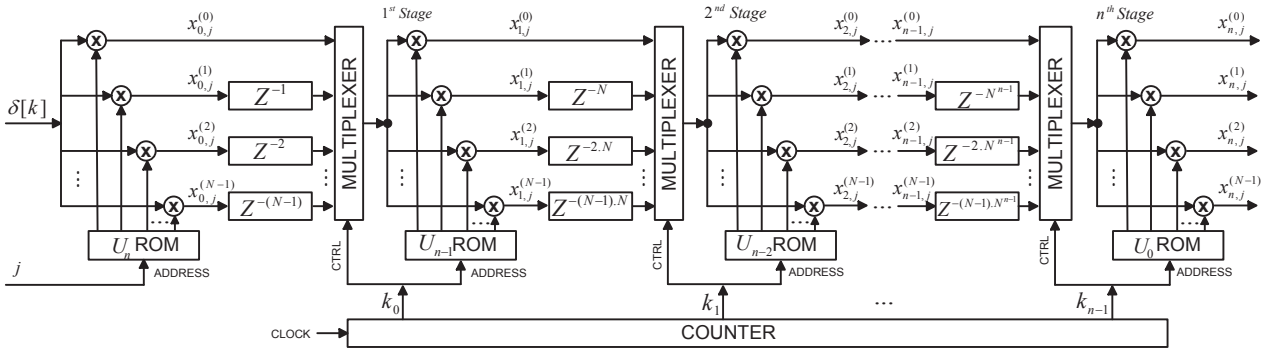

Fig. 1. The PU generator with multiplexers and ROMs for polyphase CSS.

where k has digits $k_0, k_1, \cdots, k_{r-1}$ in N-ary expansion. We can see that the expressions (23) and (35) are same. Therefore, we have the following proposition.

Proposition 4: The proposed PU generator with multiplexers and ROMs (Fig. 1) is equivalent to the generator given by (19).

C. Implementation without Multipliers

Since the signals are polyphase having constant amplitude and no addition is to be performed, we can represent them by their phases. In fact, we need only $log_2(T)$ bits for $T = 2^t$ phases. In this case, the multipliers are replaced by adders and ROMs store the phases of unitary matrix elements instead of complex values. At the output of the generator, we need to add a converter from phase values to complex values in order to get the complex signals. The proposed PU generator without multiplier is shown in Fig. 2. According to Fig. 2, we need $N(n+1)$ adders, n multiplexers and 1 n-bit counter for CSS of length N^n.

D. Comparison of Construction Complexity

As far as the implementation proposed, a significant reduction of construction complexity is achieved compared to [9], [12]- [14]. It should be noted that [9], [12]-[14] use multipliers and adders, whereas the proposed implementation requires no multiplier for computation in the construction of the sequences. We shall use the (NAND) gate-count as the measure of circuit complexity. However, we will consider only the special case when $N = 2^m$, $\mathcal{L} = 2^l$ and $T = 2^t$, where $\mathcal{L}$ is the number of bits and T is the number of phases.

According to the method discussed in [9], it requires $N^3 + N^4 + \cdots + N^{n+2} = N^3(N^n - 1)/(N - 1)$ complex multiplications to construct CCC of length N^n starting with CCC of length N^2. It is well known that complex multiplication requires four real multiplications and two real additions. Also complex addition requires two real additions. Therefore, it requires $4N^3(N^n - 1)/(N - 1)$ real multiplications and $2N^3(N^n - 1)/(N - 1)$ real additions for CCC of length N^n. On the other hand, we can observe that the straightforward implementation (19) requires $4N^3(n+1)$ multipliers and $2N^2(2N-1)(n+1)$ adders for CCC of length N^n. TABLE II shows the gate-count needed for the construction of CCC with length N^n between the straightforward implementation (19), N-CO-CCC [9] and the proposed multiplier-free implementation Fig. 2. In the comparison, we have used the estimates given by: $\mathcal{L}$-bit adder $\approx 9\mathcal{L}$ gates, $\mathcal{L}$-bit counter $\approx 9\mathcal{L}$ gates and $\mathcal{L}$-bit multiplexer $(N:1) \approx 4(N-1)\mathcal{L}$ gates [23].

TABLE II
GATE-COUNT NEEDED FOR CCC OF LENGTH N^n

N-CO-CCC [9]		Straightforward (19)	Fig. 2
$(N, n, \mathcal{L})$		$(N, n, \mathcal{L})$	(N, n, T)
	gate-count	gate-count	gate-count
Add.	$\frac{18N^3(N^n-1)}{N-1}\mathcal{L}$	$18N^2(2N-1)(n+1)\mathcal{L}$	$9N^2(n+1)t$
Mult.	$\frac{36N^3(N^n-1)}{N-1}\mathcal{L}^2$	$36N^3(n+1)\mathcal{L}^2$	0
MUX	0	0	$4Nn(N-1)t$
CNTR	0	0	$9nlog_2(N)$

V. CONCLUSION

In this paper, we have proposed a new generator for CCCs of length N^n ($n \in \mathbb{N}$) based on paraunitary matrices of size $N \times N$. We have shown that the proposed algorithm can generate N-CO-CCCs of length N^n ($n > 1$). Next, we have introduced a new PU generator for CSS. Our proposed algorithm for CSS is implemented by using multiplexers and ROMs. This allows us to generate CCCs without using multipliers. As multipliers are avoided, substantial reduction of construction complexity for CCCs is obtained as compared to the existing works. Therefore, the CCCs constructed by the proposed algorithm may be used in interference-free MC-CDMA system with low implementation cost.

ACKNOWLEDGMENT

The work of S. Das and S. Majhi was supported by the Ministry of Human Resource Development, Government of India. The work of S. Budišin was partially supported by the Ministry of Education and Science of the Republic of Serbia under the Project TR-36029, year 2015.

REFERENCES

[1] C. D. Marziani, J. Ureña, Á. Hernandez, and et al., "Acoustic sensor network for relative positioning of nodes," *Sensors*, vol. 9, no. 11, pp. 8490–8507, 2009.

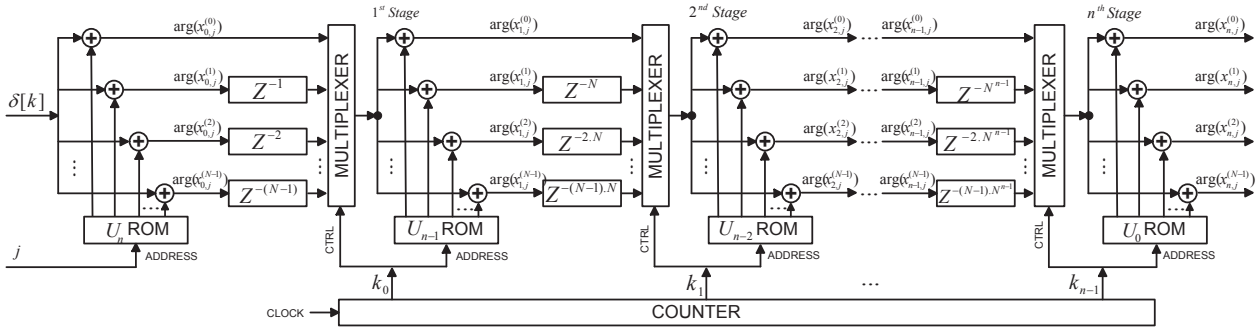

Fig. 2. The proposed PU generator with multiplexers and ROMs for polyphase CSS without multipliers.

[2] H.-H. Chen, J.-F. Yeh, and N. Suehiro, "A multicarrier CDMA architecture based on orthogonal complementary codes for new generations of wideband wireless communications," *IEEE Commun. Mag.*, vol. 39, no. 10, pp. 126–135, Oct. 2001.

[3] M. E. Magaña, T. Rajatasereekul, D. Hank, and H. H. Chen, "Design of an MC-CDMA system that uses complete complementary orthogonal spreading codes," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 2976–2989, Sep. 2007.

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

[5] X. Tang, P. Fan, and J. Lindner, "Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4038–4045, Aug. 2010.

[6] Z. Liu, Y. L. Guan, and U. Parampalli, "A new construction of zero correlation zone sequences from generalized Reed-Muller codes," in *Proc. IEEE Inf. Theory Workshop (ITW 2014)*, Nov. 2014, pp. 591–595.

[7] E. Garcia, J. Urena, J. J. Garcia, M. C. Perez, and D. Ruiz, "Efficient generator/correlator of GPC sequences for QS-CDMA," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1676–1679, Oct. 2012.

[8] C. C. Tseng and C. L. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory*, vol. 18, no. 5, pp. 644–652, Sep. 1972.

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

[10] N. Suehiro and N. Kuroyanagi, "Multipath-tolerant binary signal design for approximately synchronized CDMA systems without co-channel interference using complete complementary codes," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM 1998)*, vol. 3, Nov. 1998, pp. 1356–1361.

[11] N. Suehiro, N. Kuroyanagi, T. Imoto, and S. Matsufuji, "Very efficient frequency usage system using convolutional spread time signals based on complete complementary code," in *Proc. IEEE Int. Symp. on Personal Indoor and Mobile Radio Commun.. (PIMRC'00)*, vol. 2, Sep. 2000, pp. 1567–1572.

[12] C. Han and N. Suehiro, "A generation method for constructing (N,N,MN/P) complete complementary sequences," in *Proc. of the Joint IST Workshop on Mobile Future and Symposium on Trends in Communications (SympoTIC04)*, Oct. 2004, pp. 70–73.

[13] C. Han, N. Suehiro, and T. Hashimoto, "N-shift cross-orthogonal sequences and complete complementary codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2611–2615.

[14] ——, "A systematic framework for the construction of optimal complete complementary codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6033–6042, Sep. 2011.

[15] X. Yang, Y. Mo, D. Li, and M. Bian, "New complete complementary codes and their analysis," in *Proc. IEEE Globe Telecommun. Conf. (GLOBECOM 2007)*, Nov. 2007, pp. 3899–3904.

[16] A. Rathinakumar and A. K. Chaturvedi, "Complete mutually orthogonal Golay complementary sets from Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1339–1346, Mar. 2008.

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

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

[19] 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.

[20] H. H. Chen, S. W. Chu, and M. Guizani, "On next generation CDMA technologies: the REAL approach for perfect orthogonal code generation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 5, pp. 2822–2833, Sep. 2008.

[21] Z. Liu, Y. L. Guan, and W. H. Mow, "A tighter correlation lower bound for quasi-complementary sequence sets," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 388–396, Jan. 2014.

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

[23] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolic, *Digital Integrated Circuits*. Englewood Cliffs, Prentice Hall, 2002, vol. 2.