Asymptotically Optimal and Near-optimal Aperiodic Quasi-Complementary Sequence Sets Based on Florentine Rectangles

Avik Ranjan Adhikary, Member, IEEE, Yanghe Feng, Zhengchun Zhou, Member, IEEE, and Pingzhi Fan, Fellow, IEEE.

Abstract

Quasi-complementary sequence sets (QCSSs) can be seen as a generalized version of complete complementary codes (CCCs), which enables multicarrier communication systems to support more users. The contribution of this work is two-fold. First, we propose a systematic construction of Florentine rectangles. Secondly, we propose several sets of CCCs and QCSS, using Florentine rectangles. The CCCs and QCSS are constructed over $\mathbb{Z}_N$, where $N \geq 2$ is any integer. The cross-correlation magnitude of any two of the constructed CCCs is upper bounded by $N$. By combining the proposed CCCs, we propose asymptotically optimal and near-optimal QCSSs with new parameters. This solves a long-standing problem, of designing asymptotically optimal aperiodic QCSS over $\mathbb{Z}_N$, where $N$ is any integer.

Index Terms

Asymptotically optimal quasi-complementary sequence set (QCSSs), Complete complementary codes (CCCs), Florentine rectangles.

I. INTRODUCTION

Golay complementary pairs (GCPs) were proposed by M. J. Golay in 1951 in his work on multislit spectrometry [1]. Golay complementary pairs are a pair of sequences whose aperiodic...
autocorrelations sum up to zero at each non-zero time shift [1], [2]. In 1972, Tseng and Liu extended the concept from complementary pairs to complementary sets (CS) [3]. In a remarkable work in 1988, Suehiro and Hatori proposed N-shift cross orthogonal sequences [4], which were later termed as perfect complementary sequence sets (PCSS). A set of $K$ mutually orthogonal CS, where each CS consists of $M$ sequences (also known as sub-carriers), each of length $N$, is called a $(K, M, N)$-PCSS. PCSSs are also known as mutually orthogonal Golay complementary sets (MOGCS) [5]. Owing to their ideal correlation properties, PCSSs have been widely used in multi-carrier code division multiple access (MC-CDMA) systems for the reduction of the peak-to-average power ratio (PAPR) [6], channel estimation [7], [8], etc. One of the main drawbacks of PCSS with $M$ sub-carriers is that, when used in MC-CDMA systems, it can support at most $M$ users [10], [11].

Working towards the goal of enabling MC-CDMA systems to support more users, Liu et al. [15] designed low correlation zone complementary sequence sets (LCZ-CSSs) in 2011. Later in 2013, Liu et al. designed quasi-complementary sequence sets (QCSSs) [16] by generalizing the concept of LCZ-CSSs. The concept of QCSS also includes Z-complementary sequence sets (ZCSSs) [17]–[23]. A QCSS of set size $K$, flock size $M$, sequence length $N$ and maximum aperiodic or periodic correlation tolerance $\delta_{\text{max}}$, is written as $(K, M, N, \delta_{\text{max}})$-QCSS. For QCSS, the set size $K$ denotes the number of users it can support, the flock size $M$ denotes the number of sub-carriers. When $K \leq M$ and the periodic or aperiodic correlation tolerance $\delta_{\text{max}} = 0$, QCSS becomes PCSS. When $K = M$, a PCSS is called a complete complementary code (CCC) [16].

The first correlation lower bound of sequences was given by Welch [24] in 1974. Later, in a series of works in 2011, 2014 and 2017 [25]–[27], Liu et al. derived some special conditions for aperiodic QCSSs and further tightened the lower bound. We call a QCSS optimal if $\delta_{\text{max}}$ achieves these lower bounds.

Systematic constructions of optimal QCSS, both periodic and aperiodic, for various parameters remains very challenging till date. In [16], Liu et al. designed periodic optimal QCSS by using Signer difference sets. Utilizing the properties of the difference sets and almost difference sets Li et al. gave systematic framework to construct periodic optimal and near-optimal QCSSs in [28], [29]. In [30] and [31], Li et al. proposed periodic QCSSs using characters over finite fields. Recently, in 2019, asymptotically optimal aperiodic QCSSs were first proposed by Li et al. [32], based on low-correlation CSSs over the alphabet $\mathbb{Z}_N$, where $N$ is a prime integer or power


TABLE I: Asymptotically optimal aperiodic QCSSs.

| References | Set Size       | Flock Size | Sequence Length | $\delta_{\text{max}}$ | Alphabet | Parameter constraint(s)                      |
|------------|----------------|------------|-----------------|-----------------------|----------|---------------------------------------------|
| [33]       | $t(t-1)$       | $t$        | $t$             | $t$                   | $\mathbb{Z}_t$| $t$ is an odd prime.                      |
| Theorem 1 [32] | $u(u+1)$ | $u$ | $u$ | $u$ | $\mathbb{Z}_u$ | $u$ is power of a prime. |
| Theorem 3 [32] | $u^2$ | $u$ | $u-1$ | $u$ | $\mathbb{Z}_u$ | $u$ is power of a prime, and $u \geq 5$. |
| [34]       | $N(t_0-1)$    | $N$        | $N$             | $N$                   | $\mathbb{Z}_N$| $N$ is odd, $N \geq 5$, and $t_0$ is the smallest prime factor of $N$. |
| Proposed   | $N \times F(N)$ | $N$ | $N$ | $N$ | $\mathbb{Z}_N$ | $N \geq 2$ is any integer. |

of a prime integer. In [33], Li et al. designed a systematic framework to construct aperiodic asymptotically optimal QCSSs using several sets of CCCs having prime length sequences over the alphabet $\mathbb{Z}_N$, where $N$ is a prime integer. Recently in 2020, Zhou et al. [34] proposed a general construction of QCSS over $\mathbb{Z}_N$, for any odd integer $N \geq 3$. Asymptotically optimal aperiodic QCSSs with corresponding parameters, reported till date, are given in Table I.

Analysing closely the results of [32], [33] and [34] it is being observed that the number of CCC’s and eventually the set size of the QCSS are small when $N$ is 3 or have the smallest prime factor 3. Also it has been observed in all the previous constructions [32]–[34] that the optimal QCSS are designed over $\mathbb{Z}_N$, where $N$ always a prime, power of prime or an odd integer, depending on the constructions. To overcome these problems, in search of new approaches to design QCSSs over any alphabet size $N$, we propose several sets of CCCs and eventually QCSSs using Florentine rectangles.

Florentine rectangles are extensively studied since 1989 [12]–[14]. Almost all of the studies are focused on searching the existence of Florentine rectangles of given orders. Also, most of the available examples are based on computer search results. To the best of the authors’ knowledge systematic constructions of Florentine rectangles are available for few particular orders of Florentine rectangles only. To construct the CCCs and eventually the QCSS, in this paper, we give a systematic construction of Florentine rectangle having a flexible order. The proposed method drastically improves the set size of the QCSS, including the cases when $N$ have the smallest prime factor 3. The proposed construction generates multiple CCCs and eventually asymptotically optimal QCSSs over $\mathbb{Z}_N$, where $N$ is any even integer, like $N = 6, 10$, etc. To the best of the authors knowledge, QCSSs over any alphabet size $N$ are not reported before. The construction uses the intrinsic structural properties of Florentine rectangles to construct these CCCs and
QCSSs. Using the proposed framework, several sets of CCCs having parameters \((N, N, N)\) are proposed. Further, utilizing the constructed CCCs, we propose \((N \times F(N), N, N, N)\)-QCSS, where \(F(N) \times N\) Florentine rectangles exist. Since for \(F(N) \geq 3\) (except when \(N = 2\) and \(3\)), the proposed QCSS have set size \((K) \geq 3M\), flock size \((M) \geq 2\) and sequence length \((N) \geq 2\), we will check the optimality condition using the the correlation lower bound given by Liu et al. in [26]. The cross-correlation magnitude among the CCCs is upper bounded by \(N\). The optimality factor \(\rho\) of the proposed QCSSs, obtained by combining the CCCs, are approximately equal to 1, hence resulting asymptotically optimal QCSSs. For the cases when \(N = 2\) and \(3\), we use the Welch bound [24] to calculate the optimality factor \(\rho\).

The rest of this paper is organized as follows. In Section II, we recall some definitions and correlation bounds related to QCSS. In Section III, we recall the definitions of Florentine rectangles and Vatican squares. We also give some systematic constructions of Florentine rectangles and Vatican squares in this section. In Section IV, we have utilised the permutations, obtained from the Florentine rectangles, to construct several sets of CCCs. In Section V, we construct QCSS by combining the several sets of CCCs. In Section VI, we have made a comparison of our construction with the previous constructions reported in the literature. Finally, we conclude our paper in Section VII.

II. PRELIMINARIES

Before we begin, let us define the notations that we will be using in the paper.

- \(N\) is an integer.
- Let the ring of integers modulo \(N\) be denoted by \(\mathbb{Z}_N\).
- \(\omega_N = e^{\frac{2\pi i}{N}}\) is a primitive \(N\)-th root of unity.
- Let a set of sequence sets be denoted by \(\mathcal{C}\).
- A sequence set be denoted by \(\mathcal{C}\).
- A sequence be denoted by \(C\).
- The complex conjugate of \(x\) is denoted by \(x^*\).

**Definition 1:** Let \(C = (c_0, c_1, \cdots, c_{N-1})\) and \(D = (d_0, d_1, \cdots, d_{N-1})\) be two length \(N\) complex-valued sequences. The aperiodic correlation function (ACF) between \(C\) and \(D\) is defined as

\[
\tilde{R}_{C,D}(\tau) = \begin{cases} 
\sum_{t=0}^{N-1-\tau} c_t d_{t+\tau}^*, & 0 \leq \tau \leq N - 1 \\
\sum_{t=0}^{N-1+\tau} c_{t-\tau} d_t^*, & -N + 1 \leq \tau < 0 
\end{cases}.
\]  

October 22, 2020 DRAFT
Definition 2: Consider $\mathcal{C} = \{C^0, C^1, \ldots, C^{K-1}\}$, consisting $K$ sequence sets, each having $M$ sequences of length $N$, i.e.,

$$C^k = \begin{bmatrix}
C^k_0 \\
C^k_1 \\
\vdots \\
C^k_{M-1}
\end{bmatrix}_{M \times N}$$

where $C^k_m$ is the $m$-th sequence of length $N$ and is expressed as $C^k_m = (c^k_{m,0}, c^k_{m,1}, \ldots, c^k_{m,N-1})$, $0 \leq m \leq M-1$. The set $\mathcal{C}$ is called a $(K, M, N, \delta_{\text{max}})$ quasi-complementary sequence set (QCSS) if for any $C^{k_1}, C^{k_2} \in \mathcal{C}$, $0 \leq k_1, k_2 \leq K-1$, $0 \leq \tau \leq N-1$, $k_1 \neq k_2$ or $0 < \tau \leq N-1$, $k_1 = k_2$,

$$|\tilde{R}_{C^{k_1}, C^{k_2}}(\tau)| = \left| \sum_{m=0}^{M-1} \tilde{R}_{C^k_m, C^k_m}(\tau) \right| \leq \delta_{\text{max}},$$

where $K$, $M$, $N$ and $\delta_{\text{max}}$ denotes the set size, the number of sequences in each sequence set, the length of constituent sequences, and the maximum aperiodic cross-correlation magnitude of $\mathcal{C}$, respectively. When $K = M$ and $\delta_{\text{max}} = 0$, $(K, M, N, \delta_{\text{max}})$-QCSS transforms into $(M, M, N)$-CCC.

We now discuss the lower bound of $\delta_{\text{max}}$.

Lemma 1: [24] Considering aperiodic correlation, for a QCSS with set size $K$, flock size $M$, sequence length $N$ and aperiodic correlation tolerance $\delta_{\text{max}}$, the following inequality holds

$$\delta_{\text{max}} \geq MN \cdot \sqrt{\frac{(K^2 - 1)}{K(2N^2 - 1)}}.$$  \hspace{1cm} (4)

In 2014, Liu et al. [26] proposed a tighter lower bound of $\delta_{\text{max}}$ for aperiodic QCSS by imposing certain restrictions on the values of $K$, $M$ and $N$.

Lemma 2: [26] For an aperiodic QCSS with set size $K$, flock size $M$, sequence length $N$ and aperiodic correlation tolerance $\delta_{\text{max}}$, the following inequality holds

$$\delta_{\text{max}} \geq \sqrt{MN \left( 1 - 2 \sqrt{\frac{M}{3K}} \right)};$$  \hspace{1cm} (5)

when $K \geq 3M$, $M \geq 2$ and $N \geq 2$.

In this work, when $K \geq 3M$, i.e., for $F(N) \geq 4$, a QCSS is optimal if $\delta_{\text{max}}$ satisfies (5) with equality. Therefore, when $K \geq 3M$, the optimality factor $\rho$ is defined as follows

$$\rho = \frac{\delta_{\text{max}}}{\sqrt{MN \left( 1 - 2 \sqrt{\frac{M}{3K}} \right)}}.$$  \hspace{1cm} (6)
When $K \geq 3M$, i.e., when $F(N) < 4$, we define the optimality factor $\rho$ as

$$\rho = \frac{\delta_{\text{max}}}{MN \cdot \sqrt{\frac{K}{K(2N-1)}}} \quad (7)$$

In general, $\rho \geq 1$. When $\rho = 1$, a QCSS is said to be optimal. A QCSS is near-optimal when $1 < \rho \leq 2$.

**III. FLORENTINE RECTANGLES AND VATICAN SQUARES. ITS EXISTENCE AND CONSTRUCTIONS**

In this section we will revisit the definition and existence of Florentine rectangles and Vatican squares. We will also go through some of the constructions of Florentine rectangles and Vatican squares.

**Definition 3:** A Tuscan-$k$ rectangle of order $r \times N$ has $r$ rows and $N$ columns such that

C1: each row is a permutation of the $N$ symbols and

C2: for any two distinct symbols $a$ and $b$ and for each $1 \leq m \leq k$, there is at most one row in which $b$ is $m$ steps to the right of $a$.

When $k = N - 1$, it is called Tuscan-$(N - 1)$ rectangle or Florentine rectangle. When $r = N$ and $k = N - 1$, it is called Tuscan-$(N - 1)$ squares or Florentine squares.

**Definition 4 (Latin Square):** A matrix $A$ of size $N \times N$ is called a Latin square if each row and each column of $A$ contains the $N$ symbols, say $0, 1, \ldots, N - 1$, exactly once.

**Definition 5:** An $N \times N$ Florentine square is called Vatican square if it is also Latin.

**Example 1:** Examples of $4 \times 4$ Vatican square and $6 \times 7$ Florentine rectangle are given below in the form of matrices, respectively.

$$
\begin{bmatrix}
0, & 1, & 3, & 2 \\
1, & 2, & 0, & 3 \\
2, & 3, & 1, & 0 \\
3, & 0, & 2, & 1
\end{bmatrix}
, \quad
\begin{bmatrix}
0, & 1, & 2, & 3, & 4, & 5, & 6 \\
0, & 2, & 4, & 6, & 1, & 3, & 5 \\
0, & 3, & 6, & 2, & 5, & 1, & 4 \\
0, & 4, & 1, & 5, & 2, & 6, & 3 \\
0, & 5, & 3, & 1, & 6, & 4, & 2 \\
0, & 6, & 5, & 4, & 3, & 2, & 1
\end{bmatrix}.
$$

(8)

As we see, C1 and C2 of Definition 3 hold here.

For each positive integer $N$ let $F(N)$ denote the largest integer such that Florentine rectangle of order $F(N) \times N$ exists.
TABLE II: Possible values of $F(N)$ for $0 < N \leq 32$ [13].

| $N$ | Possible value of $F(N)$ | $N$ | Possible value of $F(N)$ |
|-----|-------------------------|-----|-------------------------|
| 1   | 1                       | 17  | 16, 17                  |
| 2   | 2                       | 18  | 18                      |
| 3   | 2                       | 19  | 18, 19                  |
| 4   | 4                       | 20  | 6, ..., 20              |
| 5   | 4                       | 21  | 6, ..., 21              |
| 6   | 6                       | 22  | 22                      |
| 7   | 6                       | 23  | 22, 23                  |
| 8   | 7                       | 24  | 6, ..., 24              |
| 9   | 8                       | 25  | 6, ..., 25              |
| 10  | 10                      | 26  | 6, ..., 26              |
| 11  | 10                      | 27  | 6, ..., 27              |
| 12  | 12                      | 28  | 28                      |
| 13  | 12, 13                  | 29  | 28, 29                  |
| 14  | 6, ..., 14              | 30  | 30                      |
| 15  | 6, ..., 15              | 31  | 30, 31                  |
| 16  | 16                      | 32  | 6, ..., 32              |

There are very few constructions of Florentine rectangles reported in literature. All the reported constructions of the Florentine rectangles are mostly based on extensive computer search. Much of the research reported in the literature is on finding the existence of an $F(N) \times N$ Florentine rectangle for a given $N$. Based on that, for a given value of $0 < N \leq 32$, we have given the probable value of $F(N)$, in Table II, for which an $F(N) \times N$ Florentine rectangle can exist.

Lemma 3 (Construction of Vatican squares): Let $p$ be an odd prime integer. Then the multiplication table of $\mathbb{Z}_p$, without the border consisting of all-zero row and column, is a $(p-1) \times (p-1)$ Vatican square. This also implies that for $N = p - 1$, where $p$ is an odd prime, $F(N) = p - 1$.

Theorem 1: Let $\mathcal{M}$ be a multiplication table of the elements of $\mathbb{Z}_N$ with the first row $M_{0,j} = 0$ for all $0 \leq j < N$ and the first column $M_{i,0} = 0$ for all $0 \leq i < N$. $M_{1,j} = j$ for all $0 \leq j < N$ and $M_{i,1} = i$ for all $0 \leq i < N$. Let $0 < i < p$, $\mathcal{A} = [M_{i,\cdot}]$, where $p$ is the smallest prime factor of $N$. Then $\mathcal{A}$ is a $(p-1) \times N$ Florentine rectangle.

Proof: Let the element $b$ be $m$ steps right to $a$ in two rows $r_1$ and $r_2$ of the matrix $\mathcal{A}$,
for some \( r_1 \neq r_2, a \neq b \). Let us assume that \( a \) is in the \( A_{r_1,c_1} \) and \( A_{r_2,c_2} \) positions, for some columns \( c_1 \) and \( c_2 \) of \( A \). Therefore, according to our assumptions \( b \) will be in positions \( A_{r_1,c_1+m} \) and \( A_{r_2,c_2+m} \), respectively. Since \( A \) is a multiplication table of the residue of \( \mathbb{Z}_N \), so we have the following:

\[
a \equiv r_1 \cdot c_1 \equiv r_2 \cdot c_2 \pmod{N}. \tag{9}
\]

Similarly, we also have

\[
b \equiv r_1 \cdot (c_1 + m) \equiv r_2 \cdot (c_2 + m) \pmod{N}. \tag{10}
\]

As per our construction \( A_{r_1,1} = r_1 \) and \( A_{r_2,1} = r_2 \). Since \( r_1 \) and \( r_2 \) are non-zero residues and prime to \( N \) therefore their inverses exist in \( \mathbb{Z}_N \). From (9) we have

\[
c_1 \equiv r_1^{-1} \cdot a \pmod{N},
\]

and

\[
c_2 \equiv r_2^{-1} \cdot a \pmod{N}. \tag{11}
\]

Replacing the value of \( c_1 \) and \( c_2 \) in (10) we have

\[
b \equiv r_1 \cdot (r_1^{-1} \cdot a + m) \pmod{N},
\]

and

\[
also, b \equiv r_2 \cdot (r_2^{-1} \cdot a + m) \pmod{N}. \tag{12}
\]

Since \( m \not\equiv 0 \pmod{N} \), therefore from (12) we have,

\[
r_1 m \equiv r_2 m \pmod{N}
\]

\[
\implies r_1 \equiv r_2 \pmod{N}. \tag{13}
\]

Since \( r_1 \) and \( r_2 \) are less than \( p \), the smallest prime factor of \( N \), therefore (13) implies \( r_1 = r_2 \), or in other words, \( r_1 \) and \( r_2 \) are same row, which contradicts our assumption. Hence \( A \) is a \((p - 1) \times N\) Florentine rectangle.

**Theorem 2:** Let \( N \geq 4, N = 2m \) and \( m \not\equiv 1 \pmod{3} \). Let \( A \) be a \( 4 \times N \) matrix and \( A_{i,j} \) denotes the \( j \)-th element of the \( i \)-th row. Define \( A_{i,j} \) as follows:

\[
A_{0,j} = \begin{cases} 
    j \pmod{N+1}, & \text{for } 1 \leq j \leq m; \\
    (N+1) - A_{0,N+1-j} \pmod{N+1} & \text{for } m+1 \leq j \leq N;
\end{cases} \tag{14}
\]

\[
A_{1,j} = \begin{cases} 
    2j \pmod{N+1}, & \text{for } 1 \leq j \leq m; \\
    (N+1) - A_{1,N+1-j} \pmod{N+1} & \text{for } m+1 \leq j \leq N;
\end{cases} \tag{15}
\]

October 22, 2020
for $i = 2$ and $i = 3$,

$$A_{i,j} = A_{3-i,N+1-j}, \text{ for } 1 \leq j \leq N. \quad (16)$$

Then $\mathcal{A}$ is a $4 \times N$ Florentine rectangle.

\textbf{Proof:} Let the element $b$ be $k$ steps right to $a$ in two rows $r_1$ and $r_2$ of the matrix $\mathcal{A}$, for some $r_1 \neq r_2$, $a \neq b$. Let us assume that $a$ is in the $A_{r_1,c_1}$ and $A_{r_2,c_2}$ positions, for some columns $c_1$ and $c_2$ of $\mathcal{A}$. Therefore, according to our assumptions $b$ will be in positions $A_{r_1,c_1+k}$ and $A_{r_2,c_2+k}$, respectively.

Let us consider $r_1 = 0$ and $r_2 = 1$, i.e., consider the positions of $a$ and $b$ in the first and second row. When $r_1 = 0$, if $1 \leq c_1 \leq m$ then $a = c_1 \pmod{N + 1}$, if $m < c_1 \leq N$ then $a = (N + 1) - (N + 1) + c_1 \pmod{N + 1} = c_1 \pmod{N + 1}$. According to our assumption in row $r_1 = 0$, $b$ will be in position $A_{0,c_1+k}$. For $r_1 = 0$, when $1 < c_1 + k \leq m$ then $b = c_1 + k \pmod{N + 1}$, when $m < c_1 + k \leq N$ then $b = (N + 1) - (N + 1) + (c_1 + k) \pmod{N + 1} = c_1 + k \pmod{N + 1}$.

When $r_2 = 1$, if $1 \leq c_2 \leq m$ then $a = 2c_2 \pmod{N + 1}$, if $m < c_2 \leq N$ then $a = (N + 1) - 2(N + 1) + 2c_2 \pmod{N + 1} = 2c_2 \pmod{N + 1}$. According to our assumption in row $r_2 = 1$, $b$ will be in position $A_{1,c_2+k}$. For $r_2 = 1$, when $1 < c_2 + k \leq m$ then $b = 2(c_2 + k) \pmod{N + 1}$, when $m < c_2 + k \leq N$ then $b = (N + 1) - 2(N + 1) + 2(c_1 + k) \pmod{N + 1} = 2(c_1 + k) \pmod{N + 1}$.

Following the above detail explanation there will be sixteen sub-cases. The first sub-case is when $c_1 \leq m$, $c_1 + k \leq m$, $c_2 \leq m$, and $c_2 + k \leq m$. In this case, we have

$$a \equiv c_1 \equiv 2c_2 \pmod{N + 1}, \quad (17)$$

and

$$b \equiv c_1 + k \equiv 2(c_2 + k) \pmod{N + 1}. \quad (18)$$

Combining (17) and (18), we get

$$k \equiv 2k \pmod{N + 1}, \quad (19)$$

which is impossible, since $N \geq 4$ and $k \geq 1$. Similarly we can prove the other sub-cases. Also similar proof can be given for other values of $r_1$ and $r_2$. Hence $\mathcal{A}$ is a $4 \times N$ Florentine rectangle.
**Theorem 3:** Let \( N \geq 4 \), \( N = 2m \) and \( m \not\equiv 0 \) (mod 3). Let \( A \) be a \( 4 \times N \) matrix and \( A_{i,j} \) denotes the \( j \)-th element of the \( i \)-th row. Define \( A_{i,j} \) as follows:

\[
A_{0,j} = \begin{cases} 
  j, & \text{for } 1 \leq j \leq m; \\
  (N + 1) - A_{0,N+1-j}, & \text{for } m + 1 \leq j \leq N; 
\end{cases} 
\quad (20)
\]

\[
A_{1,j} = \begin{cases} 
  1 + \{[2(i - 1) + m - 1] \pmod{N}\}, & \text{for } 1 \leq j \leq m; \\
  (N + 1) - A_{1,N+1-j}, & \text{for } m + 1 \leq j \leq N; 
\end{cases} 
\quad (21)
\]

for \( i = 2 \) and \( i = 3 \),

\[
A_{i,j} = A_{3-i,N+1-j}, \quad \text{for } 1 \leq j \leq N. \quad (22)
\]

Then \( A \) is a \( 4 \times N \) Florentine rectangle.

**Proof:** Let the element \( b \) be \( k \) steps right to \( a \) in two rows \( r_1 \) and \( r_2 \) of the matrix \( A \), for some \( r_1 \neq r_2 \), \( a \neq b \). Let us assume that \( a \) is in the \( A_{r_1,c_1} \) and \( A_{r_2,c_2} \) positions, for some columns \( c_1 \) and \( c_2 \) of \( A \). Therefore, according to our assumptions \( b \) will be in positions \( A_{r_1,c_1+k} \) and \( A_{r_2,c_2+k} \), respectively.

Let us consider \( r_1 = 0 \) and \( r_2 = 1 \), i.e., consider the positions of \( a \) and \( b \) in the first and second row. When \( r_1 = 0 \), if \( 1 \leq c_1 \leq m \) then \( a = c_1 \), if \( m < c_1 \leq N \) then \( a = (N + 1) - (N + 1) + c_1 = c_1 \). According to our assumption in row \( r_1 = 0 \), \( b \) will be in position \( A_{0,c_1+k} \). For \( r_1 = 0 \), when \( 1 < c_1 + k \leq m \) then \( b = c_1 + k \), when \( m < c_1 + k \leq N \) then \( b = (N + 1) - (N + 1) + (c_1 + k) = c_1 + k \).

When \( r_2 = 1 \), if \( 1 \leq c_2 \leq m \) then \( a = 1 + \{[2(c_2 - 1) + m - 1] \pmod{N}\} \), if \( m < c_2 \leq N \) then \( a = (N + 1) - 1 - \{[2(N + 1 - c_2 - 1) + m - 1] \pmod{N}\} = N - \{[2(N - c_2) + m - 1] \pmod{N}\} \). According to our assumption in row \( r_2 = 1 \), \( b \) will be in position \( A_{1,c_2+k} \). For \( r_2 = 1 \), when \( 1 < c_2 + k \leq m \) then \( b = 1 + \{[2(c_2 + k - 1) + m - 1] \pmod{N}\} \), when \( m < c_2 + k \leq N \) then \( b = (N + 1) - 1 - \{[2(N + 1 - c_2 - k - 1) + m - 1] \pmod{N}\} = N - \{[2(N - c_2 - k) + m - 1] \pmod{N}\} \).

Following the above detail explanation there will be sixteen sub-cases. The first sub-case is when \( c_1 \leq m \), \( c_1 + k \leq m \), \( c_2 \leq m \), and \( c_2 + k \leq m \). In this case, we have

\[
a \equiv c_1 \equiv 1 + \{[2(c_2 - 1) + m - 1] \pmod{N}\}, \quad (23)
\]
and
\[ b \equiv c_1 + k \equiv 1 + \left\{ [2(c_2 + k - 1) + m - 1] \pmod{N} \right\} \]
\[ \Rightarrow c_1 + k - 1 \equiv \left\{ \left[ [2(c_2 - 1) + m - 1] \pmod{N} \right] \right. \\
\left. + 2k \pmod{N} \right\} \pmod{N} \]  \hspace{1cm} (24)

From (23) we can write (24) as
\[ c_1 + k - 1 \equiv \left\{ [(c_1 - 1) + 2k] \pmod{N} \right\} \pmod{N}. \]  \hspace{1cm} (25)

Since \( c_1 + k \leq m \), therefore \( 2k \pmod{N} = 2k \), and hence (25) can be written as
\[ c_1 + k - 1 \equiv \left\{ [(c_1 - 1) + 2k] \pmod{N} \right\} \]
\[ \Rightarrow c_1 - 1 + 2k = NQ + c_1 + k - 1, \]  \hspace{1cm} (26)

For some integer \( Q \), and hence
\[ k = NQ, \]  \hspace{1cm} (27)

which is impossible, since \( k < N \). Hence our assumption is impossible. Similarly we can prove the other sub-cases. Also similar proof can be given for other values of \( r_1 \) and \( r_2 \). Hence \( A \) is a \( 4 \times N \) Florentine rectangle.

**Corollary 1:** Let \( N = 2m + 1 \). Using Theorem 2 and Theorem 3, we can construct a \( 4 \times N \) Florentine rectangle for this case also, just by adding a column of all \( N \)'s at the end of the rectangle.

**Remark 1:** For a given \( N \), the values given in Table II are higher. However, systematic construction of Florentine rectangles of order \( F(N) \times N \), when \( F(N) \) achieves the maximum value, is only available when \( N = p \) or \( N = p - 1 \), where \( p \) is prime. Computer search results of Florentine rectangles of order \( F(N) \times N \), are available for small values of \( N \). Although Theorem 1, Theorem 2, Theorem 3 or Corollary 1 do not always results to maximum number of rows for a given \( N \) which one can obtain by a computer search, we will use these results to construct the Florentine rectangles, since these are systematic constructions.

**Remark 2:** For a given \( N \), in this paper, we consider the value of \( F(N) \) as the largest integer for which we can systematically construct a Florentine rectangle of size \( F(N) \times N \). The Florentine rectangles are constructed as per following:

1) For \( N = p - 1 \), where \( p \) is prime, we construct the permutations as per Lemma 3, and then subtracting 1 from each of the elements. Therefore \( F(p - 1) = p - 1 \).
2) For $N = p$, where $p$ is prime, we first construct the Vatican square as per Lemma 3 and then add zero column in the left side of the Vatican square. Therefore $F(p) = p - 1$.

3) Let $N > 5$ be any number where $N = p^r_0 p^1_1 \ldots p^r_{n-1}$ and $p_0$ be the least prime factor of $N$. We also consider $N+1$, where $N + 1 = e_0^{s_0} e_1^{s_1} \ldots e_{m-1}^{s_m}$ and $e_0$ is the least prime factor of $N + 1$. Assume $p_0 \neq 2, 3$ and $e_0 \neq 2, 3$. If $p_0 > e_0$, we follow Theorem 1 to construct the Florentine rectangle and eventually the permutations over $N$. Therefore $F(N) = p_0 - 1$. If $p_0 < e_0$, we follow Theorem 1 to construct the Florentine rectangle and eventually the permutations over $N + 1$. Then we remove the all zero column from the rectangle and subtract 1 from each element. Therefore, $F(N) = e_0 - 1$.

4) For any positive integer $N$ having the least prime factor 2 or 3 and does not fall under above three cases, we follow Theorem 2, Theorem 3 or Corollary 1. Therefore, $F(N) = 4$. The value of $F(N)$ considered in this paper is strictly based on the above set of rules.

IV. MULTIPLE CCCs FROM FLORENTINE RECTANGLES

In this section, first we analyse some intrinsic properties of the Florentine rectangles and then we will utilise those properties to construct several sets of CCCs with low inter-set cross-correlation magnitude. Let us begin by recalling the following property of the Florentine rectangles.

**Property 1:** Let $A$ be a $F(N) \times N$ Florentine rectangle over $\mathbb{Z}_N$, denoted as follows

$$A = \begin{bmatrix}
A_{0,0}, \ldots, A_{0,N-1} \\
A_{1,0}, \ldots, A_{1,N-1} \\
\vdots \\
A_{F(N)-1,0}, \ldots, A_{F(N)-1,N-1}
\end{bmatrix}_{F(N) \times N}, \quad (28)$$

where $A_{i,j}$ denotes the $j$-th element in the $i$-th row. According to Definition 3, each row of $A$, i.e., $A_i$, is a permutation on $\mathbb{Z}_N$. Also, for each $0 < \alpha < N$, $(A_{i,j}, A_{i,j+\alpha}) \neq (A_{m,n}, A_{m,n+\alpha})$ unless $i = m$ and $j = n$, where $0 \leq i, m \leq F(N) - 1$, $0 \leq j, n \leq N - 1$, $0 < j + \alpha < N$ and $0 < n + \alpha < N$. In other words, if $\pi_i : \mathbb{Z}_N \to \mathbb{Z}_N$ be a permutation on $\mathbb{Z}_N$, where $\pi_i$ is equivalent to the $i$-th row of $A$, i.e. $A_i$, then for each $0 < \alpha < N$ $(\pi_i(j), \pi_i(j+\alpha)) = (\pi_m(n), \pi_m(n+\alpha))$ if and only if $i = m$ and $j = n$, where $0 < j + \alpha < N$ and $0 < n + \alpha < N$.

**Lemma 4:** Let $\pi_i : \mathbb{Z}_N \to \mathbb{Z}_N$ be a permutation over $\mathbb{Z}_N$ as defined in Property 1. For $0 \leq i \neq m \leq F(N) - 1$, $\pi_i(j) = \pi_m(j + \tau)$, where $0 \leq j + \tau < N$, has at most one solution for $0 \leq \tau < N$. 

October 22, 2020
Proof: Let us assume that for $0 \leq i \neq m \leq F(N) - 1$, $\pi_i(j) = \pi_m(j + \tau)$, where $0 \leq j + \tau < N$, has more than one solution for $0 \leq \tau < N$. Let two of the solutions be $j_1$ and $j_2$. Then $\pi_i(j_1) = \pi_m(j_1 + \tau)$ and $\pi_i(j_2) = \pi_m(j_2 + \tau)$. Therefore, we have $(\pi_i(j_1), \pi_i(j_2)) = (\pi_m(j_1 + \tau), \pi_m(j_2 + \tau))$. This contradicts the definition of Florentine rectangles. Hence, $\pi_i(j) = \pi_m(j + \tau)$ has at most one solution for each $0 < \tau < N$ for $0 \leq i \neq m \leq F(N) - 1$. ■

The following example illustrates the set of permutations on $\mathbb{Z}_N$ defined by the Florentine rectangles.

Example 2: Consider $N = 4$. From Example 1, we have $\pi_0(\mathbb{Z}_4) = \{0, 1, 3, 2\}$, $\pi_1(\mathbb{Z}_4) = \{1, 2, 0, 3\}$, $\pi_2(\mathbb{Z}_4) = \{2, 3, 1, 0\}$, $\pi_3(\mathbb{Z}_4) = \{3, 0, 2, 1\}$.

Utilizing the set of permutations defined in Property 1, we design several sets of CCCs using the construction framework given below.

Construction 1: Consider any positive integer $N \geq 2$, for which an $F(N) \times N$ Florentine rectangle $A$ exists over $\mathbb{Z}_N$. Also let $\pi_k$ be the permutation over $\mathbb{Z}_N$ for $0 \leq k < F(N)$, defined as above, which satisfies Lemma 4. Then for each $m \in \mathbb{Z}_N$, and $s \in \mathbb{Z}_N$, define $f_s^{(k,m)} : \mathbb{Z}_N \to \mathbb{Z}_N$ as follows

$$f_s^{(k,m)}(t) = s \cdot \pi_k(t) + mt \pmod{N}.$$  

(29)

For each $0 \leq k < F(N)$, define a set

$$\mathcal{C}^k = \{C^{(k,0)}, C^{(k,1)}, \ldots, C^{(k,N-1)}\},$$  

(30)

where

$$C^{(k,m)} = \begin{bmatrix}
C_0^{(k,m)} \\
C_1^{(k,m)} \\
\vdots \\
C_{N-1}^{(k,m)}
\end{bmatrix} = \begin{bmatrix}
C_0^{(k,m)}, C_1^{(k,m)}, \ldots, C_{N-1}^{(k,m)} \\
C_0^{(k,m)}, C_1^{(k,m)}, \ldots, C_{N-1}^{(k,m)} \\
\vdots \\
C_0^{(k,m)}, C_1^{(k,m)}, \ldots, C_{N-1}^{(k,m)}
\end{bmatrix}$$

and

$$C_{s,t}^{(k,m)} = \omega_t^{f_s^{(k,m)}(t)}$$ for each $0 \leq t \leq N - 1$.

For the sequence sets obtained using Construction 1, we have the following theorem.

Theorem 4: For $0 \leq k < F(N)$, let $\mathcal{C}^k$ be the multiple sequence sets obtained from Construction 1 based on the function $f_s^{(k,m)} : \mathbb{Z}_N \to \mathbb{Z}_N$, as given in (29). Then,

1) For each $0 \leq k < F(N)$, $\mathcal{C}^k$ is an $(N, N, N)$-CCC.
2) For any two different CCCs $\mathcal{C}^{k_1}$ and $\mathcal{C}^{k_2}$, the inter-set cross-correlation is upper bounded by $N$, i.e.,

\[
\left| \sum_{s=0}^{N-1} \tilde{R}_{\mathcal{C}_1^{(k_1,m_1)},\mathcal{C}_2^{(k_2,m_2)}}(\tau) \right| \leq N,
\]

for all $0 \leq k_1 \neq k_2 < F(N)$, $0 \leq \tau \leq N - 1$, and $0 \leq m_1, m_2 \leq N - 1$.

Proof: The proof is given in Appendix A. \hfill \blacksquare

Example 3: Let $N = 10$, The family of permutations being defined as in the first rule of Remark 2. Then we have

\[
\begin{align*}
\pi_0(\mathbb{Z}_{10}) &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}, \\
\pi_1(\mathbb{Z}_{10}) &= \{1, 3, 5, 7, 9, 0, 2, 4, 6, 8\}, \\
\pi_2(\mathbb{Z}_{10}) &= \{2, 5, 8, 0, 3, 6, 9, 1, 4, 7\}, \\
\pi_3(\mathbb{Z}_{10}) &= \{3, 7, 0, 4, 8, 1, 5, 9, 2, 6\}, \\
\pi_4(\mathbb{Z}_{10}) &= \{4, 9, 3, 8, 2, 7, 1, 6, 0, 5\}, \\
\pi_5(\mathbb{Z}_{10}) &= \{5, 0, 6, 1, 7, 2, 8, 3, 9, 4\}, \\
\pi_6(\mathbb{Z}_{10}) &= \{6, 2, 9, 5, 1, 8, 4, 0, 7, 3\}, \\
\pi_7(\mathbb{Z}_{10}) &= \{7, 4, 1, 9, 6, 3, 0, 8, 5, 2\}, \\
\pi_8(\mathbb{Z}_{10}) &= \{8, 6, 4, 2, 0, 9, 7, 5, 3, 1\}, \\
\pi_9(\mathbb{Z}_{10}) &= \{9, 8, 7, 6, 5, 4, 3, 2, 1, 0\}.
\end{align*}
\]

By Theorem 4, we get ten $(10, 10, 10)$-CCCs, $\mathcal{C}^0, \mathcal{C}^1, \mathcal{C}^2, \mathcal{C}^3, \mathcal{C}^4, \mathcal{C}^5, \mathcal{C}^6, \mathcal{C}^7, \mathcal{C}^8, \mathcal{C}^9$. The two CCCs $\mathcal{C}^2$ and $\mathcal{C}^3$ are shown in Table III.

We propose a framework to systematically construct asymptotically optimal aperiodic QCSSs, in the following section.

V. PROPOSED CONSTRUCTION OF ASYMPTOTICALLY OPTIMAL QCSSS

Theorem 5: Consider $N$ to be any positive integer greater than 3, for which $F(N) > 4$. Also, let $\mathcal{C}^k$ for $0 \leq k < F(N)$ be obtained using Theorem 4 and $\mathcal{C} = \mathcal{C}^0 \cup \mathcal{C}^1 \cup \ldots \cup \mathcal{C}^{F(N)-1}$, then the sequence set $\mathcal{C}$ is an asymptotically optimal aperiodic $(N \times F(N), N, N, N)$-QCSS.

Proof: Based on Theorem 4, for each $0 \leq k < F(N)$, $\mathcal{C}^k$ is an $(N, N, N)$-CCC. Also, for any two $k_1, k_2$, where $0 \leq k_1, k_2 < F(N)$ and $k_1 \neq k_2$, the the inter-set cross-correlation
TABLE III: The two $(10, 10, 10)$-CCCs $\mathcal{C}^2$ and $\mathcal{C}^3$ of Example 3.

| $\mathcal{C}^{(2,0)}$ | $\mathcal{C}^{(2,1)}$ | $\mathcal{C}^{(2,2)}$ | $\mathcal{C}^{(2,3)}$ | $\mathcal{C}^{(2,4)}$ | $\mathcal{C}^{(2,5)}$ | $\mathcal{C}^{(2,6)}$ | $\mathcal{C}^{(2,7)}$ | $\mathcal{C}^{(2,8)}$ | $\mathcal{C}^{(2,9)}$ |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 0.0000000000         | 0.123456789           | 0.246802468           | 0.369258147           | 0.482604826           | 0.505005005           | 0.628406824           | 0.741852963           | 0.864208642           | 0.987634211           |
| 2.580369147         | 2.063715826           | 2.726616505           | 2.849571820           | 2.972583648           | 3.095369820           | 3.218258062           | 3.341193211           | 3.464185490           | 3.587177769           |
| 4.066282788         | 4.183074963           | 4.206420642           | 4.329876321           | 4.453319963           | 4.576765634           | 4.699818407           | 4.822870158           | 4.945920937           | 5.068976756           |
| 6.549873211         | 6.663333300           | 6.786787987           | 6.909154683           | 7.031521474           | 7.153888260           | 7.276255047           | 7.398621834           | 7.520988621           | 7.643355408           |
| 8.020246468         | 8.143692147           | 8.266048826           | 8.389494505           | 8.512939184           | 8.636373863           | 8.759808542           | 8.883243221           | 8.906677900           | 9.020112579           |
| 10.500550500       | 10.623951284          | 10.746307963          | 10.869753642          | 10.992193211          | 11.114632890          | 11.237075569          | 11.360518248          | 11.483960927          | 11.607403606          |
| 13.000306960       | 13.113585660          | 13.226864340          | 13.339143020          | 13.451421699          | 13.563700379          | 13.676079059          | 13.788457739          | 13.900826428          | 14.013195108          |

Magnitude between $\mathcal{C}^{k_1}$ and $\mathcal{C}^{k_2}$ is upper bounded by $N$. Then $\mathcal{C}$ is an aperiodic $(K, M, N, \delta_{\text{max}})$-QCSS, where $K = N \times F(N)$, $M = N$, $N = N$, $\delta_{\text{max}} = \max\{0, N\} = N$.

The optimality factor of $(N \times F(N), N, N, N)$-QCSS is

$$\rho = \frac{N}{\sqrt{N^2(1 - 2\sqrt{\frac{N}{3N \times F(N)}})}}. \tag{33}$$

When $N \to +\infty$ then $F(N) \to +\infty$. Therefore from (33),

$$\lim_{F(N) \to +\infty} \rho = \lim_{F(N) \to +\infty} \frac{N}{\sqrt{N^2(1 - 2\sqrt{\frac{N}{3N \times F(N)}})}} = \lim_{F(N) \to +\infty} \frac{1}{\sqrt{1 - \frac{2}{\sqrt{3N \times F(N)}}}} \tag{34}$$

$$= 1.$$

Therefore, $\mathcal{C}$ is an asymptotically optimal aperiodic QCSS.

October 22, 2020

DRAFT
Example 4: The ten \((10, 10, 10)\)-CCCs, \(\mathcal{C}^0, \mathcal{C}^1, \mathcal{C}^2, \mathcal{C}^3, \mathcal{C}^4, \mathcal{C}^5, \mathcal{C}^6, \mathcal{C}^7, \mathcal{C}^8, \mathcal{C}^9\), generated in Example 3 can be used to construct asymptotically optimal \((100, 10, 10)\)-QCSS \(\mathcal{C} = \mathcal{C}^0 \cup \mathcal{C}^1 \cup \mathcal{C}^2 \cup \mathcal{C}^3 \cup \mathcal{C}^4 \cup \mathcal{C}^5 \cup \mathcal{C}^6 \cup \mathcal{C}^7 \cup \mathcal{C}^8 \cup \mathcal{C}^9\).

The asymptotically optimal aperiodic QCSSs obtained using Theorem 5 for some \(N\), are shown in Table IV, with corresponding parameters.

| Alphabet | \(K\) | \(M\) | \(N\) | \(\rho\) |
|----------|-------|-------|-------|--------|
| \(Z_6\)  | 36    | 6     | 6     | 1.3754 |
| \(Z_{10}\)| 100   | 10    | 10    | 1.2551 |
| \(Z_{12}\)| 144   | 12    | 12    | 1.2247 |
| \(Z_{18}\)| 324   | 18    | 18    | 1.1722 |
| \(Z_{22}\)| 484   | 22    | 22    | 1.1518 |
| \(Z_{28}\)| 784   | 28    | 28    | 1.1310 |
| \(Z_{30}\)| 900   | 30    | 30    | 1.1257 |
| \(Z_{36}\)| 1296  | 36    | 36    | 1.1128 |
| \(Z_{40}\)| 1600  | 40    | 40    | 1.1061 |
| \(Z_{42}\)| 1764  | 42    | 42    | 1.1031 |
| \(Z_{46}\)| 2116  | 46    | 46    | 1.0978 |
| \(Z_{48}\)| 288   | 48    | 48    | 1.3754 |
| \(Z_{52}\)| 2704  | 52    | 52    | 1.0912 |
| \(Z_{58}\)| 3364  | 58    | 58    | 1.0857 |
| \(Z_{60}\)| 3600  | 60    | 60    | 1.0841 |
| \(Z_{66}\)| 4356  | 66    | 66    | 1.0797 |
| \(Z_{70}\)| 4900  | 70    | 70    | 1.0771 |
| \(Z_{72}\)| 5184  | 72    | 72    | 1.0759 |
| \(Z_{76}\)| 456   | 76    | 76    | 1.3754 |
| \(Z_{78}\)| 6084  | 78    | 78    | 1.0726 |
| \(Z_{82}\)| 6724  | 82    | 82    | 1.0706 |
| \(Z_{88}\)| 7744  | 88    | 88    | 1.0679 |
| \(Z_{90}\)| 540   | 90    | 90    | 1.3754 |
| \(Z_{96}\)| 9216  | 96    | 96    | 1.0647 |
| \(Z_{100}\)| 10000 | 100   | 100   | 1.0633 |
TABLE V: Near-optimal aperiodic QCSSs, when $N$ is even number.

| Alphabet | $K$ | $M$ | $N$ | $\rho$ |
|----------|-----|-----|-----|--------|
| $\mathbb{Z}_{14}$ | 56  | 14  | 14  | 1.5382 |
| $\mathbb{Z}_{20}$ | 80  | 20  | 20  | 1.5382 |
| $\mathbb{Z}_{24}$ | 96  | 24  | 24  | 1.5382 |
| $\mathbb{Z}_{26}$ | 104 | 26  | 26  | 1.5382 |
| $\mathbb{Z}_{36}$ | 144 | 36  | 36  | 1.5382 |
| $\mathbb{Z}_{38}$ | 152 | 38  | 38  | 1.5382 |
| $\mathbb{Z}_{44}$ | 176 | 44  | 44  | 1.5382 |
| $\mathbb{Z}_{50}$ | 200 | 50  | 50  | 1.5382 |

TABLE VI: Comparison of the parameters of QCSS when the smallest prime factor of $N$ is 3.

| Alphabet | $K$ | $K_{\text{prev}}$ | $M$ | $N$ | $\rho$ | $\rho_{\text{prev}}$ |
|----------|-----|------------------|-----|-----|--------|---------------------|
| $\mathbb{Z}_{3\times5}$ | 60  | 30              | 15  | 15  | 1.5382 | 1.9653             |
| $\mathbb{Z}_{3\times7}$ | 84  | 42              | 21  | 21  | 1.5382 | 1.9755             |
| $\mathbb{Z}_{3\times11}$ | 132 | 66              | 33  | 33  | 1.5382 | 1.9846             |
| $\mathbb{Z}_{3\times5\times7}$ | 420 | 210             | 105 | 105 | 1.5382 | 1.9952             |
| $\mathbb{Z}_{3\times5\times11}$ | 660 | 330             | 165 | 165 | 1.5382 | 1.9970             |
| $\mathbb{Z}_{3\times5\times7\times11}$ | 4620 | 2310             | 1155 | 1155 | 1.5382 | 1.9996             |
| $\mathbb{Z}_{3\times5\times7\times11\times13}$ | 60060 | 30030             | 15015 | 15015 | 1.5382 | 2.0000             |
| $\mathbb{Z}_{3\times5\times7\times11\times13\times17}$ | 1021020 | 510510             | 255255 | 255255 | 1.5382 | 2.0000             |

**Corollary 2:** For the cases when $F(N) = 4$, $\mathcal{C}$ is an aperiodic near-optimal $(4N, N, N, N)$-QCSS.

**Proof:** From (33), we get

$$\rho = \frac{N}{\sqrt{N^2(1 - 2\sqrt{\frac{N}{3xN\times4}})}} = 1.5382. \quad (35)$$

**Corollary 3:** Let $N = 2$ or 3. Also, let $\mathcal{C}^0$, $\mathcal{C}^1$ be obtained from Theorem 4 and $\mathcal{C} = \mathcal{C}^0 \cup \mathcal{C}^1$. Then $\mathcal{C}$ is a near-optimal aperiodic $(4, 2, 2, 2)$-QCSS or $(6, 3, 3, 3)$-QCSS, with optimality factor $\rho = 1.6584$ or 1.7950, respectively. Since $K \not\leq 3M$, we have used the Welch bound, discussed in Lemma 1.
The results of the proposed systematic construction are compared with the results of the existing constructions in the following section.

VI. COMPARISON WITH PREVIOUS WORKS

The main difference of this construction with all the previous constructions is that here we can construct asymptotically optimal and near-optimal QCSS over \( \mathbb{Z}_N \) for any \( N > 3 \), whereas previously \( N \geq 5 \) was only odd integer [34], prime [32], [33] or power of prime [32]. For comparing the parameters with the existing results, in Table VI, \( K_{\text{prev}} \) and \( \rho_{\text{prev}} \) denote the previous set size and the previously reported optimality factor, respectively, of the QCSS over \( \mathbb{Z}_N \), for some values of \( N \), when \( N \) has a prime factor 3. The values of \( K_{\text{prev}} \) and \( \rho_{\text{prev}} \) are obtained from [34]. Compared with [32], [33] and [34], the uniqueness of our construction can be listed down as follows:

1) We can obtain asymptotically optimal QCSS with more flexible parameters using the proposed framework, as compared to the constructions proposed in [32], [33] and [34]. For instance, the asymptotically optimal and near-optimal QCSS over \( \mathbb{Z}_N \), where \( N \) is an even composite number and not a prime power, can only be obtained by the proposed construction till date. The parameters and the corresponding optimality factor of the asymptotically optimal QCSS for some of these \( N \) can be seen in Table IV. Also, the parameters and the corresponding optimality factors of some near-optimal QCSSs are shown in Table V, where \( N \) is even.

2) When \( N \) has the smallest prime factor 3, near-optimal aperiodic QCSS can be obtained. Compared to the results reported in [34], the obtained QCSSs display a lower optimality factor. Table VI compares the parameters for some of these values of \( N \) with the QCSS designed in [34].

VII. CONCLUSION

In this paper, we have presented a systematic construction of QCSSs with new flexible parameters based on Florentine rectangles. In the proposed construction, \( N > 3 \) can take any positive value. This construction not only fills the gap left by all the previous constructions, where \( N \) was considered odd, prime or prime powers, but also improves the optimality factor as compared with the previous constructions. We first proposed a new set of permutations on \( \mathbb{Z}_N \) based on Florentine rectangles and utilized those permutations to construct \((N, N, N)\)-CCCs.
Combining the newly constructed CCCs we have designed new sets of \((N \times F(N), N, N, N)\)-QCSS, where \(F(N)\) is the maximum number of rows for which an \(F(N) \times N\) Florentine rectangle exists. The designed QCSSs are asymptotically optimal and near-optimal with respect to the correlation bound in [26]. For \(N = 2\) and \(N = 3\), our construction results to near-optimal \((2N, N, N, N)\)-QCSS, with respect to the Welch bound [24]. We have also compared our proposed construction with the previous constructions reported in the literature. The proposed construction results to new QCSSs when over \(\mathbb{Z}_N\), when \(N > 3\) is an even integer. When \(N > 3\) is an odd integer, the set size increases and eventually the value of the optimality factor decreases, as compared to the previous constructions.

APPENDIX A

PROOF OF THEOREM 4

First, let us prove that, for \(0 \leq k < F(N)\), \(c^k\) is an \((N, N, N)\)-CCC. Let \(C^{(k,m_1)}, C^{(k,m_2)} \in c^k\), where \(0 \leq k < F(N), 0 \leq m_1, m_2 \leq N - 1\) and \(f_s^{(k,m)}(t)\) is as given in (29). Then

\[
\sum_{s=0}^{N-1} \tilde{R}_{C_s^{(k,m_1)}, C_s^{(k,m_2)}}(\tau) = \sum_{s=0}^{N-1} \sum_{t=0}^{N-1-\tau} C^{(k,m_1)}_{s,t} \cdot \left(C^{(k,m_2)}_{s,t+\tau}\right)^* \\
= \sum_{s=0}^{N-1} \sum_{t=0}^{N-1-\tau} \omega_{N}^{f_s^{(k,m_1)}(t)} \cdot \omega_{N}^{-f_s^{(k,m_2)}(t+\tau)} \\
= \sum_{s=0}^{N-1} \sum_{t=0}^{N-1-\tau} \omega_{N}^{s(\pi_k(t) - \pi_k(t+\tau)) + t(m_1 - m_2) - m_2 \tau}.
\]

(36)

Consider the following cases.

Case 1: When \(\tau = 0, m_1 = m_2\), then

\[
\sum_{s=0}^{N-1} \tilde{R}_{C_s^{(k,m_1)}, C_s^{(k,m_2)}}(0) = N^2.
\]

(37)
Case 2: When $1 \leq \tau \leq N - 1, m_1 = m_2,$
\[
\sum_{s=0}^{N-1} \tilde{R}_s^{(k,m_1)} C_s^{(k,m_2)}(\tau) = \sum_{s=0}^{N-1} \sum_{t=0}^{N-1-\tau} \omega_N^{-m_2\tau} \cdot \omega_N^{s(\pi_k(t) - \pi_k(t+\tau))} = 0. \tag{38}
\]
When $\tau \neq 0$, $\pi_k(t) \neq \pi_k(t + \tau)$ because $\pi_k(t)$ is a permutation on $\mathbb{Z}_N$. Also $N \nmid (\pi_k(t) - \pi_k(t + \tau))$ because $(\pi_k(t) - \pi_k(t + \tau) < N$. Therefore (38) holds.

Case 3: When $\tau = 0, m_1 \neq m_2,$
\[
\sum_{s=0}^{N-1} \tilde{R}_s^{(k,m_1)} C_s^{(k,m_2)}(0) = \sum_{s=0}^{N-1} \sum_{t=0}^{N-1} \omega_N^{t(m_1-m_2)} = 0. \tag{39}
\]

Case 4: When $1 \leq \tau \leq N - 1, m_1 \neq m_2,$
\[
\sum_{s=0}^{N-1} \tilde{R}_s^{(k,m_1)} C_s^{(k,m_2)}(\tau) = \sum_{s=0}^{N-1-\tau} \omega_N^{t(m_1-m_2)-m_2\tau} \cdot \sum_{s=0}^{N-1} \omega_N^{s(\pi_k(t) - \pi_k(t+\tau))} = 0. \tag{40}
\]
For $\tau \neq 0$, $\pi_k(t) \neq \pi_k(t + \tau)$, because $\pi_k(t)$ is a permutation on $\mathbb{Z}_N$. Also $N \nmid (\pi_k(t) - \pi_k(t + \tau))$ because $(\pi_k(t) - \pi_k(t + \tau) < N$. Therefore (40) holds.

From the above four cases, we conclude that $C^k$, for each $0 \leq k < F(N)$, is an $(N, N, N)$-CCC.

Now let us prove the second part that $C$ is a QCSS. Consider $C^{(k_1,m_1)} \in C^{k_1}$ and $C^{(k_2,m_2)} \in C^{k_2}$. Then, the ACF of $C^{(k_1,m_1)}$ and $C^{(k_2,m_2)}$ is given by
\[
\sum_{s=0}^{N-1} \tilde{R}_s^{(k_1,m_1)} C_s^{(k_2,m_2)}(\tau) = \sum_{s=0}^{N-1} \sum_{t=0}^{N-1-\tau} \omega_N^{f^{(k_1,m_1)}(t)} \cdot \omega_N^{-f^{(k_2,m_2)}(t+\tau)} = 0. \tag{41}
\]
Recall that permutations $\pi_{k_1}$ and $\pi_{k_2}$ satisfy Lemma 4. Therefore, $\pi_{k_1}(t) - \pi_{k_2}(t + \tau) \equiv 0 \pmod{N}$ for any $0 \leq t \leq t + \tau \leq N - 1$, $k_1 \neq k_2$ has at most one solution. Hence, if there is no solution, then $\sum_{s=0}^{N-1} \widetilde{R}_{C, \pi_{k_2}}^{(k_1, m_1)}(\tau) = 0$ due to $\sum_{s=0}^{N-1} \omega_N^s(\pi_{k_2}(t+\tau) - \pi_{k_1}(t)) = 0$. If there is one solution, say $t'$, then for $0 \leq t' \leq t' + \tau \leq N - 1$ or in other words for $0 \leq t' \leq N - 1 - \tau$, we have

$$\sum_{s=0}^{N-1} \widetilde{R}_{C, \pi_{k_2}}^{(k_1, m_1)}(\tau) = \omega_N^{-m_2 \tau} \cdot [\omega_N^{(m_1-m_2)t'} \cdot N + \sum_{0 \leq t \leq N-1-\tau, \ t \neq t'} \omega_N^{(m_1-m_2)t} \sum_{0 \leq s \leq N-1} \omega_N^{(\pi_{k_2}(t+\tau) - \pi_{k_1}(t)) \cdot s}]$$

$$= \omega_N^{-m_2 \tau + (m_1-m_2)t'} \cdot N.$$ 

Therefore, $|\sum_{s=0}^{N-1} \widetilde{R}_{C, \pi_{k_2}}^{(k_1, m_1)}(\tau)| \leq N$ for all $k_1 \neq k_2$, $0 \leq \tau \leq N - 1$ and $0 \leq m_1, m_2 \leq N - 1$.

Therefore, the theorem is proved.

REFERENCES

[1] M. J. E. Golay, “Static multislit spectrometry and its application to the panoramic display of infrared spectra,” J. Opt. Soc. Amer., vol. 41, pp. 468-472, Jul. 1951.
[2] M. Golay, “Complementary series,” IRE Trans. Inf. Theory, vol. 7, no. 2, pp. 82-87, Apr. 1961.
[3] C. Tseng and C. Liu, “Complementary sets of sequences,” IEEE Trans. Inf. Theory, vol. IT-18, pp. 644-665, 1972.
[4] N. Suehiro and M. Hatori, “N-shift cross-orthogonal sequences,” IEEE Trans. Inf. Theory, vol. IT-34, pp. 143-146, 1988.
[5] A. Rathinakumar and A. K. Chaturvedi, “Complete mutually orthogonal Golay complementary sets from Reed-Muller codes,” IEEE Trans. Inf. Theory, vol. 51, no. 3, pp. 1339-1346, 2008.
[6] 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, 1999.
[7] P. Spasojevic and C. N. Georghiade, “Complementary sequences for ISI channel estimation,” IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 2397-2417, 2001.
[8] S. Wang and A. Abdi, “MIMO ISI channel estimation using uncorrelated Golay complementary sets of polyphase sequences,” IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 3024-3039, 2007.
[9] A. Pezeshki, A. R. Calderbank, W. Moran, and S. D. Howard, “Doppler resilient Golay complementary waveforms,” IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4254-4266, 2008.
[10] Z. Liu, Y. L. Guan and U. Parampalli, “New complete complementary codes for peak-to-mean power control in multi-carrier CDMA,” IEEE Trans. Commun., vol. 62, no. 3, pp. 1105-1113, 2014.
[11] H. H. Chen, “The next generation CDMA technologies,” 1st edition. John Wiley & Sons, 2007.
[12] T. Etzion, S. W. Golomb, and H. Taylor, “Tuscan-ksquares,” Adv. Appl. Math., 10(1989), 164–174.
[13] H. Y. Song and J. H. Dinitz, “Tuscan squares,” *CRC handbook of combinatorial designs*, pp. 480–484, CRC Press, New York, 1996.

[14] H. Taylor, “Florentine rows or left-right shifted permutation matrices with cross-correlation values \( \leq 1 \),” *Discrete Math.*, 93(1991), 247–260.

[15] 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, 2011.

[16] Z. Liu, U. Parampalli, Y. L. Guan, and S. Bozetas, “Constructions of optimal and near-optimal quasi-complementary sequence sets from Singer difference sets,” *IEEE Wire. Commun. Lett.*, vol. 2, no.5, pp. 487-490, 2013.

[17] P. Ke and Z. Zhou, “A generic construction of Z-periodic complementary sequence sets with flexible flock size and zero correlation zone length,” *IEEE Signal Process. Lett.*, vol. 22, no. 9, pp. 1462-1466, 2015.

[18] Z. Liu, U. Parampalli and Y. L. Guan, “Optimal odd-length binary Z-complementary pairs,” *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5768-5781, 2014.

[19] Y. Li, C. Xu, N. Jing and K. Liu, “Constructions of Z-periodic complementary sequence set with flexible flock size,” *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 201-204, 2014.

[20] A. R. Adhikary, S. Majhi, “New construction of optimal aperiodic Z-complementary sequence sets of odd-lengths,” *Electron. Lett.*, vol. 55, no. 19, pp. 1043-1045, 2019.

[21] 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, 2018.

[22] C. Chen, “A novel construction of Z-complementary pairs based on generalized Boolean functions,” *IEEE Signal Process. Lett.*, vol. 24, no. 7, pp. 987-990, 2017.

[23] 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 Sign. Process. Lett.*, vol. 25, no. 7, pp. 970-973, 2018.

[24] L. R. Welch, “Lower bounds on the maximum cross-correlation of signals,” *IEEE Trans. Inf. Theory*, vol. IT-20, no. 3, pp. 397-399, 1974.

[25] Z. Liu, Y. L. Guan and W. H. Mow, “Improved lower bound for quasi-complementary sequence set,” *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, 2011, pp. 489-493.

[26] 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, 2014.

[27] Z. Liu, Y. L. Guan and W. H. Mow, “Asymptotically locally optimal weight vector design for a tighter correlation lower bound of quasi-complementary sequence sets,” *IEEE Trans. Signal Process.*, vol. 65, no. 12, pp. 3107-3119, 2017.

[28] Y. Li, T. Liu and C. Q. Xu, “Constructions of asymptotically optimal quasi-complementary sequence sets,” *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1516-1519, 2018.

[29] Y. Li, T. Yan and C. Lv, “Construction of a near-optimal quasi-complementary sequence set from almost difference set,” *Cryptogr. Commun.*, pp. 815-824, Jul. 2019.

[30] Y. Li, L. Y. Tian, T. Liu and C. Q. Xu, “Constructions of quasi-complementary sequence sets associated with characters,” *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4597-4608, 2019.

[31] Y. Li, L. Tian, T. Liu and C. Xu, “Two constructions of asymptotically optimal quasi-complementary sequence sets,” *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 1910-1924, 2019.

[32] Y. Li, L. Tian and C. Xu, “Constructions of asymptotically optimal aperiodic quasi-complementary sequence sets,” *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7499-7511, 2019.

[33] T. Liu, C. Xu and Y. Li, “Multiple complementary sequence sets with low inter-set cross-correlation property,” *IEEE Signal Process. Lett.*, vol. 26, no. 6, pp. 913-917, 2019.
[34] Z. Zhou, F. Liu, A. R. Adhikary and P. Fan, “A generalized construction of multiple complete complementary codes and asymptotically optimal aperiodic quasi-complementary sequence sets,” in IEEE Trans. Commun., vol. 68, no. 6, pp. 3564-3571, 2020.

[35] Z. Zhou, D. Zhang, T. Helleseth and J. Wen, “A construction of multiple optimal ZCZ sequence sets with good cross correlation,” IEEE Trans. Inf. Theory, vol. 64, no. 2, pp. 1340-1346, 2018.