Circular quasi-Florentine rectangles and its application in designing optimal polyphase sequence sets

Avik Ranjan Adhikary
Department of Mathematics
Southwest Jiaotong University
Chengdu, China
avik.adhikary@ieee.org

Zhengchun Zhou
School of Information Science and Technology
Southwest Jiaotong University
Chengdu, China
zzc@swjtu.edu.cn

Yang Yang
Department of Mathematics
Southwest Jiaotong University
Chengdu, China
yang_data@swjtu.edu.cn

Abstract

In this paper, first we introduce the concept of circular quasi-Florentine rectangles and propose circular quasi-Florentine rectangles when N is of the form p^n, where p is any prime number. Next, we design polyphase sequence sets with new parameters using the proposed circular quasi-Florentine rectangles. The proposed polyphase sequence sets are optimal with respect to the Welch bound.

1 Introduction

Circular Florentine rectangles first appeared around mid 1980's in the remarkable works of T. Etzion, S. Golomb and H. Taylor [1,2]. Circular Florentine rectangles are matrices of size $F_c(N) \times N$, where each of the N symbols $0,\ 1,\ 2, \cdots,\ N-1$ appears exactly once in each of the $F_c(N)$ rows. Additionally, for any two symbols a and b, and for each m from 1 to n, there is at most one row in which b is the m-th symbol to the right of a when the rows are considered to be circular. Several conjectures were proposed in [2] about the availability of circular Florentine rectangles for different values of N. Working towards this direction Song [3] constructed several circular Florentine rectangles through computer search. However, systematic construction of circular Florentine rectangle still remains open other than the cases when $N = p$ is a prime number [2].

Recently, circular Florentine rectangles emerge as an efficient combinatorial tool to design several sequence sets with various desired correlation properties. In two separate works, based on circular Florentine rectangles, Zhang *et al.* [4] and Song *et al.* [5] proposed polyphase sequence sets, which are asymptotically optimal with respect to the Welch bound [6]. The set size of all these sequence sets highly depends on the number of rows $F_c(N)$ of the corresponding circular Florentine rectangle. Since 1991 till date, very few research work has been reported towards the construction of circular Florentine rectangles for various values of N. Moreover, almost all the existing works are computer search results.

Recent applications of circular Florentine rectangles in desiging sequences with desired correlation properties motivates us to design circular Florentine rectangles with large number of rows for a given N. In [2] it is proved that $F_c(N) = N - 1$, when N is prime, and provided a systematic construction. It is also conjectured in [2] that when N is not prime, $F_c(N)$ cannot achieve the value $N-1$. In his work in [3], Song compiled all possible values of $F_c(N)$, when N is odd. It is also proved in [3] that for even N, $F_c(N) = 1$. In view of these facts, it is a challenging task to construct circular Florentine rectangles with large number of rows, when N is not prime. Working towards this direction, we introduce a new concept of "circular quasi-Florentine rectangles". In circular quasi-Florentine rectangles we preserve all the properies of circular Florentine rectangles other than the fact that every row contains $N - 1$ elements instead of N elements. In other words, one of the element is missing in each of the rows. We also propose a construction of circular quasi-Florentine rectangle for the cases when $N = p^n$. We show that for these cases we can obtain a maximum of $F_c^Q(N) = p^n$ rows. Also, when N is even and is of the form p^n, then also we can achieve p^n number of rows, earlier which was only one.

Next, to demonstrate the applications of the proposed circular quasi-Florentine rectangles in designing sequence sets, we propose a class of periodic polyphase sequence sets using the proposed circular quasi-Florentine rectangles. Polyphase sequence sets achieving Welch bound [6] has a rich literature. Interested readers can go through [4,7] and the references therein. In summary, polyphase sequences which achieves the Welch bound, have important applications in communication systems [8]. Recent works of Zhang *et al.* [4], Song *et al.* [5] motivates us to check the applications of the proposed circular quasi-Florentine rectangles in designing polyphase sequence sets. Interestingly, the proposed polyphase sequence sets are asymptotically optimal with respect to the Welch bound. The parameters of the asymptotically optimal periodic polyphase sequence sets proposed till date are listed in Table 1.

The rest of the paper is organised as follows. In Section 2, we fix some notations and revisit some basic definitions and Welch bound. In Section 3, we introduce the concept of "circular quasi-Florentine rectangles" and propose a construction when N is of the form of p^n, where p is any prime number. In Section 4, we propose a construction of periodic polyphase sequence set using the circular quasi-Florentine rectangles and discussed its optimality with respect to the Welch bound. Finally, we conclude the paper in Section 5.

2 Preliminaries

Let us fix the following notations before we begin:

Table 1: Polyphase sequences asymptotically achieving the Welch bound.

References	Period	$\theta_{\max}$	θ_a	Family Size	Alphabet Size	Constraint(s)
Sidelnikov [9]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	p^n	p	p is an odd prime
Welch and Scholtz [10,11]	p	$2+\sqrt{p}$	3	$p-2$	$p-1$	p is an odd prime
Cubic family by Alltop [12]	p	$\sqrt{p}$	$\sqrt{p}$	p	p	$p\geq 5$ is prime
Frank-Zadoff-Heimiller [13]	p^2	p	0	$p-1$	p	p is an odd prime
Popovic [14]	N	$\sqrt{N}$	0	$\nu(N)^{\dagger}$	N	$N=sl^2$ is odd
Kasami [15]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	p	$p=2$
Kumar and Moreno [16]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Liu and Komo [17]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Moriuchi and Imamura [18]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Jang *et al.* [19]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$p^{\frac{n}{2}}$	p	p is an odd prime
Family $\mathcal{A}$ [20,22]	p^n-1	$1+p^{\frac{n}{2}}$	$1+p^{\frac{n}{2}}$	$1+p^n$	4	$p=2$
Family $\mathcal{U}$ [21,22]	$p(p^n-1)$	$p+p^{\frac{n+1}{2}}$	$p+p^{\frac{n+1}{2}}$	p^n	4	$p=2$
Chung *et al.* [23]	p^2-p	p	p	p	p	p is an odd prime
Zhou *et al.* [7]	p^n-1	$p^{\frac{n}{2}}$	1	p^n-1	$p(p^n-1)$	p is any prime
Zhou *et al.* [7]	p^n-1	$p^{\frac{n}{2}}$	1	K	pK	p is any prime and $K\mid(p^n-1)$
Gu *et al.* [24]	p^m-1	$p^{k-1}p^{\frac{m}{2}}$	$p^{k-1}p^{\frac{m}{2}}$	$p^{km}-1$	$p^k(p^m-1)$	p is any prime, k is any integer
Zhang *et al.* [4]	N^2	N	0	$F_c(N)$	N	$F_c(N)$ is the number of rows of a circular Florentine rectangle
Proposed	$N(N-1)$	N	N	$F_c^Q(N)$	N	$F_c^Q(N)$ is the number of rows of a circular quasi-Florentine rectangle

- x^* denotes the conjugate of x.
- $\langle x\rangle_N$ denotes $x \pmod N$.

Let $\mathcal{C}=\{\mathbf{c}_i=\{c_{i,t}\}_{t=0}^{N-1}:0\leq i\leq M-1\}$ be a family of M unimodular polyphase sequences each of length N. The periodic correlation function between two sequences $\mathbf{c}_i$ and $\mathbf{c}_j$ in $\mathcal{C}$ is defined as follows:

$$\theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau)=\sum_{t=0}^{N-1}c_{i,t}c^*_{j,\langle t+\tau\rangle_N},\ 0\leq\tau\leq N-1. \tag{1}$$

when $i=j$, it is called autocorrelation, otherwise it is cross-correlation. Let us define the maximum magnitudes of the autocorrelation and cross-correlation of the sequences in $\mathcal{C}$ as follows:

$$\begin{aligned}\theta_a(\mathcal{C})&=\{\mid\theta_{\mathbf{c}_i}(\tau)\mid:0\leq i<M,0<\tau<N\},\\ \theta_c(\mathcal{C})&=\{\mid\theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau)\mid:0\leq i\neq j<M,0\leq\tau<N\}.\end{aligned} \tag{2}$$

Let $\theta_{\max}(\mathcal{C})=\max\{\theta_a(\mathcal{C}),\theta_c(\mathcal{C})\}$. Accordingly, a sequence set $\mathcal{C}$ is said to be an (M,N,θ_{max}) sequence set.

Lemma 1. *[6] Considering periodic correlation, for a sequence set $\mathcal{C}$ with M sequences, each of length N and periodic correlation tolerance $\theta_{\max}$, we have the Welch bound, as follows*

$$\theta_{\max} \geq N\sqrt{\frac{M-1}{NM-1}}. \tag{3}$$

An $(M, N, \theta_{\max})$- sequence set $\mathcal{C}$ is said to be optimal, if it satisfies the Welch bound, with equality. Therefore, we define the optimality factor ρ as follows:

$$\rho = \frac{\text{achieved } \theta_{max}}{\text{theoretical } \theta_{\max}}, \tag{4}$$

where "achieved $\theta_{\max}$" is the correlation bound achieved through the proposed constructions and "theoretical $\theta_{\max}$" is the Welch bound in Lemma 1. In general $\rho \geq 1$. When $\rho = 1$, we call the sequence set optimal.

3 Circular Quasi-Florentine Rectangles

In this section, first we propose the definition of circular quasi-Florentine rectangles, then we propose a construction of circular quasi-Florentine rectangles for the cases when N can be written in the form of p^n, where p is any prime number.

Definition 1. A matrix $\mathcal{A}$ over $\mathbb{Z}_N$ is said to be a circular quasi Florentine rectangle, if it satisfies the following two conditions:

C1: Each row contains $N-1$ symbols, where each symbol, except one, occours exactly once in each row.

C2: For any ordered pair (a, b) of two distinct symbols, and for any integer m from 1 to $N-2$, there is atmost one row in which b is m steps right of a, when steps are considered circularly.

Remark 1. The only difference of circular quasi Florentine rectangle from the circular Florentine rectangle is that, in circular Florentine rectangle, each row must contains all the elements of $\mathbb{Z}_N$, whereas in circular quasi Florentine rectangle, one element is missing in each of the rows. Please note that the missing element may be different for each of the rows.

3.1 Construction of circular quasi-Florentine rectangles

Construction 1. *Let p be prime and n be a positive integer. $\mathbb{F}_p$ denotes a finite field with p elements and $\mathbb{F}_q$ be the extension field of $\mathbb{F}_p$, where $q = p^n$. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{F}_p$. Let α be a primitive element of $\mathbb{F}_q$. The non-zero elements of $\mathbb{F}_q$ can be written in the power of α as $\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\}$. Let us define a one-to-one mapping ψ from $\mathbb{F}_q$ to $\mathbb{Z}_q$ which takes the n-tuple to decimal version of the elements in $\mathbb{Z}_q$.*

Example 1. When $p = 3$, $n = 2$, and primitive polynomial $f(x) = \alpha^2 + 2\alpha + 2$, the elements of $\mathbb{F}_9$ are

$$S = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}. \tag{5}$$

Then,

$$\psi(S) = \{0, 1, 3, 4, 7, 2, 6, 8, 5\}. \tag{6}$$

Theorem 1. *Let $\mathcal{A}$ be a matrix of order $q \times (q-1)$, defined as follows:*

$$\mathcal{A} = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,p^n-2} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,p^n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p^n-1,0} & a_{p^n-1,1} & \cdots & a_{p^n-1,p^n-2} \end{bmatrix}_{q\times(q-1)} \tag{7}$$

where,

$$A_{i,j} = \begin{cases} \psi(\alpha^j) & \text{for } i = 0; \\ \psi(\alpha^j + \alpha^{i-1}) & \text{for } 0 < i \leq q-1, \end{cases} \tag{8}$$

and ψ is a one-to-one mapping as defined in Construction 1. Then, $\mathcal{A}$ is a quasi Florentine rectangle of size $q \times (q-1)$, with $F_c^Q(q) = q$.

Proof. To show that $\mathcal{A}$ is a circular quasi Florentine rectangle, we need to prove the two conditions given in Definition 1.

α^j and α^{i-1} are both elements of $\mathbb{F}_q$ for $0 \leq i \leq (q-1)$ and $0 \leq j \leq (q-2)$, therefore $(\alpha^j + \alpha^{i-1}) \in \mathbb{F}_q$. Since, ψ is a one-to-one mapping, and $0 \leq j \leq (q-2)$, each element of $\mathbb{Z}_q$ will appear only once, and it will miss one element. Hence condition C1 of Definition 1 is satisfied.

Next, we prove C2. Let us assume that there are two elements x and y, where y is m (> 0) steps right of x, circularly, in two rows of $\mathcal{A}$, say r_1 and r_2, . In r_1-th row, let the position of x be at the $c_x^{r_1}$-th column, and y be at the $c_y^{r_1}$-th column. Similarly, in r_2-th row, let the position of x be at the $c_x^{r_2}$-th column, and y be at the $c_y^{r_2}$-th column. Let us assume $0 < r_1, r_2 \leq q-1$. The calculation will be similar if one of them is zero. So, we have

$$a_{r_1, c_x^{r_1}} = x = a_{r_2, c_x^{r_2}}, \tag{9}$$

and

$$a_{r_1, c_y^{r_1}} = y = a_{r_2, c_y^{r_2}}. \tag{10}$$

From (9), we have

$$\psi(\alpha^{c_x^{r_1}} + \alpha^{r_1-1}) = \psi(\alpha^{c_x^{r_2}} + \alpha^{r_2-1}), \tag{11}$$

since ψ is a bijection, we have

$$\alpha^{c_x^{r_1}} + \alpha^{r_1-1} = \alpha^{c_x^{r_2}} + \alpha^{r_2-1}. \tag{12}$$

Similarly, from (10), we have

$$\alpha^{c_y^{r_1}} + \alpha^{r_1-1} = \alpha^{c_y^{r_2}} + \alpha^{r_2-1}. \tag{13}$$

Therefore, from (12) and (13), we have

$$\begin{aligned} \alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{c_y^{r_1}} - \alpha^{c_y^{r_2}} \\ &= \alpha^{\langle c_x^{r_1}+m\rangle_{q-1}} - \alpha^{\langle c_x^{r_2}+m\rangle_{q-1}}. \end{aligned} \tag{14}$$

So, we have four cases:

Case 1: When $c_x^{r_1}+m < q-1$ and $c_x^{r_2}+m < q-1$. In this case, $\langle c_x^{r_1}+m\rangle_{q-1} = c_x^{r_1}+m$ and $\langle c_x^{r_2}+m\rangle_{q-1} = c_x^{r_2}+m$. Hence, from (14), we have

$$\begin{aligned} \alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{c_x^{r_1}+m} - \alpha^{c_x^{r_2}+m} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}}) \end{aligned} \tag{15}$$

Since $0 < r_1, r_2 \leq p^n - 1$ and $r_1 \neq r_2$, therefore, $\alpha^{r_1-1} \neq \alpha^{r_2-1}$. Note that $\alpha^{c_x^{r_1}} + \alpha^{r_1-1} = \alpha^{c_x^{r_2}} + \alpha^{r_2-1}$. Therefore, $\alpha^{c_x^{r_1}} \neq \alpha^{c_x^{r_2}}$. Hence, from (15), we have

$$\alpha^m = 1, \tag{16}$$

which implies $m = 0$ or $m = q-1$. If $m = 0$, then it is a contradiction, since we had assumed m is non-zero. If $m = q-1$, then $x = y$, which is also a contradiction, since $x \neq y$. Hence, C2 of Defintion 1 is satisfied.

Case 2: When $c_x^{r_1}+m > q-1$ and $c_x^{r_2}+m < q-1$. In this case $\langle c_x^{r_1}+m\rangle_{q-1} = [(c_x^{r_1}+m)-(q-1)]$ and $\langle c_x^{r_2}+m\rangle_{q-1} = c_x^{r_2}+m$. Hence, from (14), we have

$$\begin{aligned} \alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{\left[(c_x^{r_1}+m)-(q-1)\right]} - \alpha^{c_x^{r_2}+m} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}}), \end{aligned} \tag{17}$$

since, $\alpha^{(q-1)} = 1$. Hence, similar to Case 1 above, we can show the contradiction.

Case 3: When $c_x^{r_1}+m < q-1$ and $c_x^{r_2}+m > q-1$. In this case, we have from (14),

$$\begin{aligned} \alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{(c_x^{r_1}+m)} - \alpha^{\left[c_x^{r_2}+m-(q-1)\right]} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}}). \end{aligned} \tag{18}$$

Case 4: When $c_x^{r_1}+m > q-1$ and $c_x^{r_2}+m > q-1$. In this case, we have from (14),

$$\begin{aligned} \alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}} &= \alpha^{\left[(c_x^{r_1}+m)-(q-1)\right]} - \alpha^{\left[c_x^{r_2}+m-(q-1)\right]} \\ &= \alpha^m(\alpha^{c_x^{r_1}} - \alpha^{c_x^{r_2}}). \end{aligned} \tag{19}$$

For Case 3 and Case 4 the contradiction can be shown similar to Case 2.

This completes the proof. □

Example 2. When $p = 2$, $n = 3$, and primitive polynomial $f(x) = x^3 + x + 1$, using Theorem 1, we have

$$\mathcal{A} = \begin{bmatrix} 1 & 2 & 4 & 3 & 6 & 7 & 5 \\ 0 & 3 & 5 & 2 & 7 & 6 & 4 \\ 3 & 0 & 6 & 1 & 4 & 5 & 7 \\ 5 & 6 & 0 & 7 & 2 & 3 & 1 \\ 2 & 1 & 7 & 0 & 5 & 4 & 6 \\ 7 & 4 & 2 & 5 & 0 & 1 & 3 \\ 6 & 5 & 3 & 4 & 1 & 0 & 2 \\ 4 & 7 & 1 & 6 & 3 & 2 & 0 \end{bmatrix}_{8\times 7}, \tag{20}$$

which is a circular quasi-Florentine rectangle, with $F_c^Q(8) = 8$.

Property 1. *Let $N = p^n$, where p is prime and $n \geq 1$ is an integer. Let $\mathcal{A}$ be a circular quasi Florentine rectangle of size $F_c^Q(N) \times (N-1)$ over $\mathbb{Z}_N$, given as follows:*

$$\mathcal{A} = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,N-2} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,N-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{F_c^Q(N)-1,0} & a_{F_c^Q(N)-1,1} & \cdots & a_{F_c^Q(N)-1,N-2} \end{bmatrix}_{F_c^Q(N)\times(N-1)} \tag{21}$$

where $a_{i,j}$ denotes the j-th element of the i-th row. According to Definition 1, each row of $\mathcal{A}$, i.e., $\mathbf{a}_i$ for $0 \leq i < F_c^Q(N)$, is a permutation on $\mathbb{Z}_N$, missing one element. For each $0 < m < N-1$, $(a_{i,\langle j\rangle_{(N-1)}}, a_{i,\langle j+m\rangle_{(N-1)}}) \neq (a_{p,\langle q\rangle_{(N-1)}}, a_{p,\langle q+m\rangle_{(N-1)}})$ unless $i = p$ and $j = q$, where $0 \leq i, p \leq F_c^Q(N) - 1$, $0 \leq j, q \leq N-2$, $0 < \langle j+m\rangle_{(N-1)} < N-1$ and $0 < \langle q+m\rangle_{(N-1)} < N-1$. In other words, if $\pi_i^{cQ} : \mathbb{Z}_N \to \mathbb{Z}_N$ be a permutation on $\mathbb{Z}_N$, i.e., if π_i^{cQ} denotes the i-th row of $\mathcal{A}$, then for each $0 < m < N-1$, $(\pi_i^{cQ}(j), \pi_i^{cQ}(\langle j+m\rangle_{(N-1)})) = (\pi_p^{cQ}(q), \pi_p^{cQ}(\langle q+m\rangle_{(N-1)}))$ if and only if $i = p$ and $j = q$, where $0 \leq j, q < N-1$.

Lemma 2. *Let $\mathcal{A}$ be a quasi-Florentine rectangle of size $F_c^Q(N) \times (N-1)$. Let π_i^{cQ} denotes the i-th row of a quasi Florentine rectangle $\mathcal{A}$. For $0 \leq i \neq j < F_c^Q(N)$, $\pi_i^{cQ}(\langle k\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k+\tau\rangle_{(N-1)})$, has atmost one solution.*

Proof. Assume that for $0 \leq i \neq j < F_c^Q(N)$, $\pi_i^{cQ}(\langle k\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k+\tau\rangle_{(N-1)})$, has more than one solution for $0 \leq \tau < N-1$. Let k_1 and k_2 be the two solutions. Then, we have $\pi_i^{cQ}(\langle k_1\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k_1+\tau\rangle_{(N-1)})$ and $\pi_i^{cQ}(\langle k_2\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k_2+\tau\rangle_{(N-1)})$. Therefore, we have $(\pi_i^{cQ}(\langle k_1\rangle_{(N-1)}), \pi_i^{cQ}(\langle k_2\rangle_{(N-1)})) = (\pi_j^{cQ}(\langle k_1+\tau\rangle_{(N-1)}), \pi_j^{cQ}(\langle k_2+\tau\rangle_{(N-1)}))$. This contradicts the definition of circular quasi Florentine rectangles. Hence, $\pi_i^{cQ}(\langle k\rangle_{(N-1)}) = \pi_j^{cQ}(\langle k+\tau\rangle_{(N-1)})$, has at most one solution for each $0 < \tau < N-1$ for $0 \leq i \neq j < F_c^Q(N)$. □

4 Construction of asymptotically optimal polyphase sequence sets from circular quasi-Florentine rectangles

Let $\mathcal{A}$ be a circular quasi-Florentine rectangle. Then each row of a $\mathcal{A}$ is a permutation over $\mathbb{Z}_N$, missing one element, according to C1 of Defintion 1. Let the i-th row of $\mathcal{A}$ be denoted by π_i^{cQ}, then π_i^{cQ} is a permutation over $\mathbb{Z}_N$, which misses one element.

Construction 2. *Consider any positive integer $N \geq 2$, for which an $F_c^Q(N) \times (N-1)$ circular quasi-Florentine rectangle $\mathcal{A}$ exists over $\mathbb{Z}_N$. Also let π_i^{cQ} be the permutation over $\mathbb{Z}_N$ for $0 \leq i < F_c^Q(N)$, defined as above, which satisfies Lemma 2. Then for $0 \leq t < N(N-1)$, define $h_i(t)$ as follows:*

$$h_i(t) = t\pi_i^{cQ}(\langle t \rangle_{(N-1)}), \tag{22}$$

Construct a sequence set $\mathcal{C}$ of order $F_c^Q(N) \times N(N-1)$, as follows:

$$\mathcal{C}=\begin{bmatrix} \mathbf{c}_0 \\ \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_{F_c^Q(N)-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,N(N-1)-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,N(N-1)-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{F_c^Q(N)-1,0} & c_{F_c^Q(N)-1,1} & \cdots & c_{F_c^Q(N)-1,N(N-1)-1} \end{bmatrix}_{F_c^Q(N)\times N(N-1)}, \tag{23}$$

where

$$c_{i,j} = \omega_N^{h_i(j)}. \tag{24}$$

Theorem 2. *The sequence set $\mathcal{C}$, derived in Construction 2, is an $(F_c^Q(N), N(N-1), \theta_{\max})$ polyphase sequence set over $\mathbb{Z}_N$, with $\theta_{\max} = N$.*

Proof. The size of $\mathcal{C}$ is $F_c^Q(N) \times (N-1)$. For $0 \leq i, j < F_c^Q(N)$, and $0 \leq \tau < L$, where $L = N(N-1)$, we have

$$\begin{aligned} \theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) &= \sum_{k=0}^{L-1} c_{i,k} \left(c_{j,\langle k+\tau\rangle_L}\right)^* \\ &= \sum_{k=0}^{L-1} \omega_N^{h_i(k)} \left(\omega_N^{h_j(k+\tau)}\right)^* \\ &= \sum_{k=0}^{L-1} \omega_N^{k\pi_i^{cQ}(\langle k\rangle_{(N-1)})-(k+\tau)\pi_j^{cQ}(\langle k+\tau\rangle_{(N-1)})} \\ &= \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1\pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)})-\pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} \end{aligned} \tag{25}$$

where $k_0 = \langle k\rangle_{N-1}$, $k_1 = \langle k\rangle_N$, $\tau_0 = \langle \tau\rangle_{N-1}$, and $\tau_1 = \langle \tau\rangle_N$. We have the following cases:

- Case I: when $i = j$, $\tau_0 = 0$ and $\tau_1 = 0$. In this case, from (25), we have

$$\theta_{\mathbf{c}_i}(0) = N(N-1). \tag{26}$$

- Case II: when $i = j$, $\tau_0 = 0$ and $\tau_1 \neq 0$, we have from (25)

$$\theta_{\mathbf{c}_i}(\tau) = N \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1\pi_i^{cQ}(\langle k_0\rangle_{(N-1)})} \tag{27}$$

$\pi_i^{cQ}(k_0)$ is a permutation on $\mathbb{Z}_N$, missing one element, according to the construction. Let that missing element be t, then (27) becomes

$$\theta_{\mathbf{c}_i}(\tau) = N\omega_N^{-\tau_1 \cdot t}. \tag{28}$$

Therefore, in this case $\mid \theta_{\mathbf{c}_i}(\tau) \mid= N$.

- Case III: when $i = j$, $\tau_0 \neq 0$, we have from (25),

$$\theta_{\mathbf{c}_i}(\tau) = \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1 \pi_i^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)})-\pi_i^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))}. \tag{29}$$

Since $\pi_i^{cQ}(k_0)$ is a permutation missing one element, so $\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) \neq \pi_i^{cQ}(\langle k_0 + \tau_0\rangle_{(N-1)}$. Hence,

$$\sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)})-\pi_i^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} = 0. \tag{30}$$

Therefore, in this case $\mid \theta_{\mathbf{c}_i}(\tau) \mid= 0$.

- Case IV: when $i \neq j$, we have from (25),

$$\theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) = \sum_{k_0=0}^{N-2} \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)})-\pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} \tag{31}$$

Note that $\pi_i^{cQ}(\langle k_0\rangle_{(N-1)}) - \pi_j^{cQ}(\langle k_0 + \tau_0\rangle_{(N-1)}) = 0$ has atmost one solution as per Lemma 2. Therefore, if there is no solution then

$$\sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)})-\pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} = 0, \tag{32}$$

hence, $\mid \theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) \mid= 0$. However, if there is a solution, let k_0' be the solution. Then we have from (31),

$$\begin{aligned}\theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) &= N \cdot \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0'+\tau_0\rangle_{(N-1)})} \\ &\quad + \sum_{\substack{k_0=0 \\ k_0 \neq k_0'}}^{N-2} \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)})} \cdot \sum_{k_1=0}^{N-1} \omega_N^{k_1(\pi_i^{cQ}(\langle k_0\rangle_{(N-1)})-\pi_j^{cQ}(\langle k_0+\tau_0\rangle_{(N-1)}))} \\ &= N \cdot \omega_N^{-\tau_1 \pi_j^{cQ}(\langle k_0'+\tau_0\rangle_{(N-1)})}.\end{aligned} \tag{33}$$

Hence, in this case $\mid \theta_{\mathbf{c}_i,\mathbf{c}_j}(\tau) \mid= N$.

Therefore, combining all the cases, we have $\theta_{\max}(\mathcal{C}) = N$. This proves the theorem.

□

4.1 Discussion on optimality

Theorem 3. *Let $\mathcal{C}$ be the sequence sets with parameters $(F_c^Q(N), N(N-1), N)$, as proposed in Theorem 2. Then $\mathcal{C}$ is an asymptotically optimal polyphase sequence set with respect to the Welch bound.*

Proof. From (4), we have

$$\rho = \frac{N}{N(N-1)\sqrt{\frac{F_c^Q(N)-1}{N(N-1)F_c^Q(N)-1}}}. \tag{34}$$

After some routine calculation we get

$$\rho = \frac{1}{\sqrt{1-\frac{1}{N}}}\frac{\sqrt{1-\frac{1}{F_c^Q(N)N(N-1)}}}{\sqrt{1-\frac{1}{F_c^Q(N)}}} \tag{35}$$

Hence, for the cases when $N \to \infty$, $F_c^Q(N) \to \infty$, we have $\lim\limits_{N\to\infty} \rho = 1$.

Since in our case for $N = p^n$, $F_c^Q(N) = p^n$, we have $\lim\limits_{N\to\infty} \rho = 1$. Hence, the proposed sequence sets are asymptotically optimal. □

Next we give an example of the proposed polyphase sequence sets.

Example 3. Let $p = 2$, $n = 3$, then $N = 2^3 = 8$. Using the circular quasi-Florentine rectangle constructed in *Example* 2, following **Construction** 2, we obtain asymptotically optimal polyphase sequence set $\mathcal{C}$ over $\mathbb{Z}_8$ with parameters $(8, 56, 8)$. A glimpse of the periodic autocorrelation and cross-correlation among the sequences are shown in Fig. 1.

5 Conclusion

In this paper, we have introduced a new concept of circular quasi-Florentine rectangle and proposed a construction of circular quasi-Florentine rectangle of size $F_c^Q(N) \times N$ when N is of the form p^n, where p is any prime number. We have also proposed a class of polyphase sequences using the circular quasi-Florentine rectangles which are asymptotically optimal with respect to the Welch bound.

References

[1] S. Golomb, and H. Taylor. Tuscan squares-a new family of combinatorial designs. *Ars Combinatoria* 20, 115–132, 1985.

[2] T. Etzion, S. Golomb, and H. Taylor. Tuscan-k squares. *Adv. Appl. Maths* 10(2), 164–174, 1989.

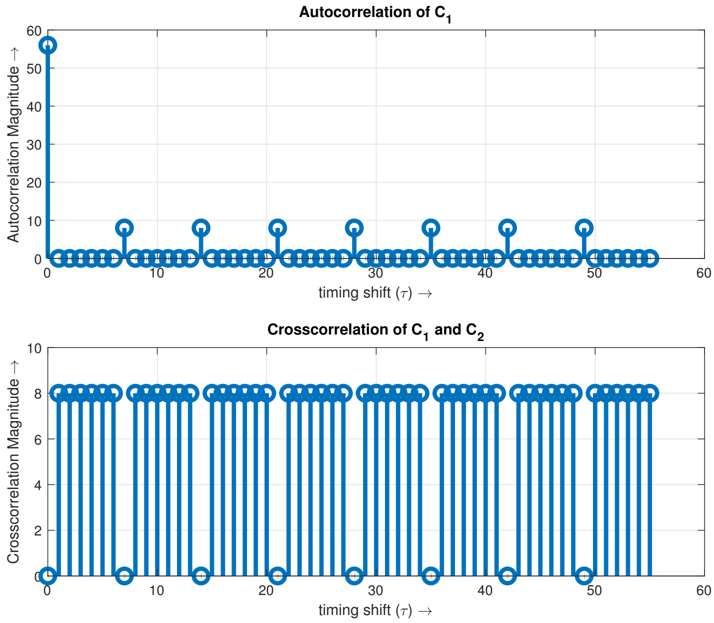

Figure 1: Glimpse of correlation magnitudes of the sequences $\mathbf{c}_1$, $\mathbf{c}_2$ of $\mathcal{C}$ in *Example 3*.

[3] H.-Y. Song. On aspects of Tuscan squares. M.S. thesis, Dept. Elect. Eng., Univ. Southern California, Los Angeles, CA, USA, 1991.

[4] D. Zhang and T. Helleseth. Sequences With Good Correlations Based on Circular Florentine Arrays. *IEEE Trans. Inf. Theory*, 68(5), 3381–3388, 2022.

[5] M. K. Song and H. -Y. Song. New Framework for Sequences With Perfect Autocorrelation and Optimal Crosscorrelation. *IEEE Trans. Inf. Theory*, 67(11), 7490–7500, 2021.

[6] L. R. Welch. Lower bounds on the maximum cross correlation of signals (Corresp.). *IEEE Trans. Inf. Theory*, IT-20(3), 397–399, 1974.

[7] Z. Zhou, T. Helleseth and U. Parampalli. A Family of Polyphase Sequences With Asymptotically Optimal Correlation. *IEEE Trans. Inf. Theory*, 64(4), 2896–2900, 2018.

[8] S. W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar.* Cambridge, U.K.: Cambridge Univ. Press, 2005.

[9] V. M. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl.*, 12, 197–201, 1971.

[10] R. A. Scholtz and L. R. Welch. Group characters: Sequences with good correlation properties. *IEEE Trans. Inf. Theory*, IT-24(5), 537–545, 1978.

[11] K.-U. Schmidt. Sequence families with low correlation derived from multiplicative and additive characters. *IEEE Trans. Inf. Theory*, 57(4), 2291–2294, 2011.

[12] W. O. Alltop. Complex sequences with low periodic correlations (Corresp.). *IEEE Trans. Inf. Theory*, IT-26(3), 350–354, 1980.

[13] R. L. Frank, S. A. Zadoff, and R. Heimiller. Phase shift pulse codes with good periodic correlation properties (Corresp.). *IRE Trans. Inf. Theory*, IT-8(6), 381–382, 1962.

[14] B. M. Popovic. Generalized chirp-like polyphase sequences with optimum correlation properties. *IEEE Trans. Inf. Theory*, 38(4), 1406–1409, 1992.

[15] T. Kasami. Weight distribution formula for some class of cyclic codes. Coordinated Sci. Lab., Univ. Illinois Urbana–Champaign, Urbana, IL, USA, Tech. Rep. R-285 (AD632574), 1966.

[16] P. V. Kumar and O. Moreno. Prime-phase sequences with periodic correlation properties better than binary sequences. *IEEE Trans. Inf. Theory*, 37(3), 603–616, 1991.

[17] S.-C. Liu and J. J. Komo. Nonbinary Kasami sequences over GF(p). *IEEE Trans. Inf. Theory*, 38(4), 1409–1412, 1992.

[18] T. Moriuchi and K. Imamura. Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar–Moreno sequences. *IEEE Trans. Inf. Theory*, 41(2), 572–576, 1995.

[19] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth. New family of p-ary sequences with optimal correlation property and large linear span. *IEEE Trans. Inf. Theory*, 50(8), 1839–1843, 2004.

[20] S. Boztas, R. Hammons, and P. Y. Kumar. 4-phase sequences with near-optimum correlation properties. *IEEE Trans. Inf. Theory*, 38(3), 1101–1113, 1992.

[21] X. H. Tang and P. Udaya. A note on the optimal quadriphase sequences families. *IEEE Trans. Inf. Theory*, 53(1), 433–436, 2007.

[22] P. Udaya and M. U. Siddiqi. Optimal and suboptimal quadriphase sequences derived from maximal length sequences over Z4. *Appl. Algebra Eng., Commun. Comput.*, 9(2), 161–191, 1998.

[23] J.-H. Chung and K. Yang. A new class of balanced near-perfect nonlinear mappings and its application to sequence design. *IEEE Trans. Inf. Theory*, 59(2), 1090–1097, 2013.

[24] Z. Gu, Z. Zhou, S. Mesnager, P. Udaya. A new family of polyphase sequences with low correlation. *Cryptogr. Commun.* 14, 135–144, 2022.