A New Family of Perfect Polyphase Sequences with Low Cross-Correlation

Dan Zhang
Norwegian university of science and technology
Email: dan.zhang@ntnu.no

Staal Amund Vinterbo
Norwegian university of science and technology
Email: staal.vinterbo@ntnu.no

Abstract—Spread spectrum multiple access systems demand minimum possible cross-correlation between the sequences within a set of sequences having good auto-correlation properties. Through a connection between generalised Frank sequences and Florentine arrays, we present a family of perfect sequences with low cross-correlation having a larger family size, compared with previous works. In particular, the family size can be equal to the square root of the period when the period of the perfect sequences is even. In contrast, the number of the perfect sequences of even period with low cross-correlation is equal to one in all previous works.

Index terms—Perfect sequences, perfect auto-correlation, low cross-correlation, Florentine arrays, polyphase sequences.

I. Introduction

Sequences and their properties have been widely studied in different research areas because many applications depend on their characteristics. Sequences with desirable correlation properties have been used in communication systems and radar systems for identification, synchronization, ranging, and interference mitigation [?]. In Code-Division Multiple-Access systems, low cross-correlation between the desired and interfering users is important to suppress multi-user interference. Good auto-correlation properties are important for reliable initial synchronization and separation of the multi-path components. Moreover, the number of available sequences should be sufficiently large so that it can accommodate enough users. Therefore, it is of great interest to design families of sequences with large family size and low correlation.

The periodic *cross-correlation* value of two complex sequences $\mathbf{u} = \{u(t)\}_{t=0}^{N-1}$ and $\mathbf{v} = \{v(t)\}_{t=0}^{N-1}$ of period N at shift τ is defined as

$$R_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{t=0}^{N-1} u(t+\tau)v^*(t), \qquad 0 \le \tau < N,$$

where N is a positive integer, $t+\tau$ is taken modulo N, and $v^*(t)$ is the complex conjugate of the complex number $v(t)$. When sequences $\mathbf{u}$ and $\mathbf{v}$ are identical, the periodic cross-correlation function is called *auto-correlation* function, and is denoted by $R_{\mathbf{u}}(\tau)$. A sequence is said to be *perfect* if all the out-of-phase periodic auto-correlation coefficients are zero, i.e., $R_{\mathbf{u}}(\tau) = 0$ for $\tau \not\equiv 0 \mod N$.

Let $\mathcal{S}$ be a set of M sequences of period N. The maximum out-of-phase periodic auto-correlation magnitude is denoted by R_a and defined by $R_a = \max\{|R_{\mathbf{s}_i}(\tau)| : \mathbf{s}_i \in \mathcal{S}, 0 < \tau < N\}$. The maximum periodic cross-correlation magnitude is denoted by R_c and defined by $R_c = \max\{|R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| : \mathbf{s}_i \neq \mathbf{s}_j \in \mathcal{S}, 0 \le \tau < N\}$. A lower bound on $R_{\max} = \max(R_a, R_c)$ given by Welch [?] is $R_{\max} \ge N\sqrt{\frac{M-1}{MN-1}}$. Due to the above bound, it is of great interest to design a sequence set with $\sqrt{N} \le R_{\max} \le c\sqrt{N}$, where c is a small constant and N is the period of the sequences in the family. We call such a set *a family of sequences with low correlation*. Excellent surveys and fundamental discussions on this topic can be found [?], [?].

We are particularly interested in families of perfect sequences with low correlation. Perfect sequences have ideal auto-correlation, i.e., $R_a = 0$. Another bound called the Sarwate bound [?] implies that $R_c \ge \sqrt{N}$. A set of perfect sequences meeting this bound is called an *optimal* set of perfect sequences. Extensive research has been done on how to generate optimal families of perfect sequences [?], [?], [?], [?], [?], [?], [?], [?], [?]. The family size of optimal families of perfect sequences with optimal cross-correlation is equal to $p-1$, where p is the smallest prime divisor of the period N. Recent works [?], [?] show that the family size can be larger than

$p+1$, that is determined by the existence of well-studied combinatorial objects, the circular Florentine arrays. However, their constructions based on circular Florentine arrays that produce large families of perfect sequences only for odd periods. When the period is even, the constructions yield families of size one.

In this paper, we propose a construction of perfect sequences with low correlation based on the non-circular Florentine arrays. This construction allows us to derive a family of perfect sequences with $R_c = 2\sqrt{N}$ where N is the period of the sequences. The family size depends on the existence of Florentine arrays, which is greater than that in the previous works. In particular, the number of perfect sequences with low cross-correlation can be $\sqrt{N}$ for even N. Table ?? relates the above previous works to our results.

II. Preliminaries

A. Florentine arrays

An $m \times n$ (circular) Tuscan-k array has m rows and n columns such that 1) each row is a permutation of n symbols and 2) for any two symbols a and b, and for each t from 1 to k, there is at most one row in which b occurs t steps (circularly) to the right of a. In particular, a (circular) Tuscan-$(n-1)$ array is referred to as a (circular) Florentine array. When $m = n$, we call them (circular) Tuscan squares and (circular) Florentine squares, respectively.

For each positive integer $n \geq 2$, we denote $F(n)$ the maximum number such that an $F(n) \times n$ Florentine array exists and $F_c(n)$ the maximum number such that an $F_c(n) \times n$ circular Florentine array exists. By definition, $F(n) \geq F_c(n)$ for all n, because any circular Florentine arrays are also Florentine arrays.

Lemma 1. [?]

(1) $F_c(n) = 1$ when n is even, and

(2) $p - 1 \leq F_c(n) \leq n - 1$, where p is the smallest prime factor of n, and

(3) $F_c(n) = n - 1$ when n is a prime.

Lemma 2. [?]

(1) $F(n) \leq n$, and

(2) $F(n) \geq F_c(n+1)$ for all n, and

(3) $F(n) \geq n - 1$ and $F(n-1) = n - 1$ when n is a prime; and

(4) $F(n) \geq p - 1$ and $F(n-1) \geq p - 1$, where p is the smallest prime divisor of n.

Note that the fact that $F(n) \geq F_c(n+1)$ for all n, is because any $F_c(n+1)$ circular Florentine rows on $n+1$ symbols can lead to the same number of rows on n symbols by deleting any one symbol in each row. With this fact and the lower bound on $F_c(n)$, one can derive both $F(n) \geq p-1$ and $F(n-1) \geq p-1$, where p is the smallest prime divisor of n. It follows that $F(n) \geq n-1$ and $F(n-1) = n-1$ when n is a prime.

TABLE I: 6×6 and 6×7 Florentine arrays [?]

0	2	1	4	5	3
1	3	2	5	0	4
2	4	3	0	1	5
3	5	4	1	2	0
4	0	5	2	3	1
5	1	0	3	4	2

1	2	3	4	5	6	0
2	5	0	4	3	1	6
3	0	1	4	6	5	2
5	3	6	4	0	2	1
6	1	5	4	2	0	3
0	6	2	4	1	3	5

To achieve the upper bound on $F(n)$, it will be interesting to know when a Florentine square exists. The only known Florentine squares of order n are Vatican squares and come form the so-called prime construction which essentially is from the multiplication table mod $(n+1)$, where $n+1$ is prime. Exhaustive search for Florentine arrays has been done by many researchers. Taylor [?] gave a table of all possible values of $F(n)$ for $1 \leq n \leq 32$, which was later updated by Hong Yeop Song [?] (See Table ??). For more works on Tuscan arrays, see [?], [?].

TABLE II: Possible values of $F(n)$ [?]

n	$F(n)$	n	$F(n)$	n	$F(n)$
1	1	11	10	21	$7, \cdots, 21$
2	2	12	12	22	22
3	2	13	12, 13	23	22, 23
4	4	14	$7, \cdots, 14$	24	$6, \cdots, 24$
5	4	15	$7, \cdots, 15$	25	$6, \cdots, 25$
6	6	16	16	26	$6, \cdots, 26$
7	6	17	16, 17	27	$6, \cdots, 27$
8	7	18	18	28	28
9	8	19	18, 19	29	28, 29
10	10	20	$6, \cdots, 20$	30	30

Let C be an $m \times n$ Florentine array on $\mathbb{Z}_n$, where $\mathbb{Z}_n$ denotes the ring of integers modulo n. The rows are indexed as 1 to m. By definition, each row is a permutation over $\mathbb{Z}_n$, denoted by β_i for $1 \leq i \leq m$. These permutations have the following property.

Lemma 3. For $1 \leq i, j \leq m$ such that $i \neq j$ and $l \in \mathbb{Z}_n$, let

$$\mathcal{N}^l_{(i,j)} = \{t \in \mathbb{Z}_n \mid \beta_i(t) = \beta_j((t+l) \bmod n)\}.$$

Then $|\mathcal{N}^l_{(i,j)}| \leq 2$ and the bound is tight.

Proof. Let addition be in $\mathbb{Z}$ and let $\delta(x) = 1(x \ge n)$ where 1 is the indicator function. Which indicates whether argument x "wraps around" modulo n.

For any $l \in \mathbb{Z}_n$ and $i \neq j$, let $t, t' \in \mathcal{N}^l_{(i,j)}$ and $t \neq t'$. First we prove that $\delta(t+l) \neq \delta(t'+l)$. Without loss of generality, let $0 \le t < t' < n$. Since $t, t' \in \mathcal{N}^l_{(i,j)}$, we have

$$\beta_i(t) = \beta_j((t+l) \bmod n), \text{ and}$$
$$\beta_i(t') = \beta_j((t'+l) \bmod n)$$

We assume that $\delta(t+l) = \delta(t'+l) = c$. It follows that

$$((t'+l) \bmod n) - ((t+l) \bmod n)$$
$$= (t'+l-cn) - (t+l-cn)$$

Then the pair $(\beta_i(t), \beta_i(t')) = (\beta_j((t+l) \bmod n), \beta_j((t'+l) \bmod n)) \triangleq (a, b)$ with b being the $(t'-t)$-th step to the right of a appear at two different rows i and j, which contradicts the definition of Florentine arrays. Therefore, $\delta(t+l) \neq \delta(t'+l)$ for $t, t' \in \mathcal{N}^l_{(i,j)}$.

Now we show that $|\mathcal{N}^l_{(i,j)}| \le 2$. Assume on the contrary, there exist $t, t', t'' \in \mathcal{N}^l_{(i,j)}$ with $0 \le t < t' < t'' < n$. Since δ is a two-valued function, at least two of the elements $\delta(t+l)$, $\delta(t'+l)$ and $\delta(t''+l)$ must share the same value. This contradicts the fact that $\delta(t+l)$ and $\delta(t'+l)$ can not be the same for any $t, t' \in \mathcal{N}^l_{(i,j)}$. Consequently, we have $|\mathcal{N}^l_{(i,j)}| \le 2$ for $l \in \mathbb{Z}_n$ and $i \neq j$.

For the 6×6 Florentine array in Table ??, $\mathcal{N}^2_{(1,2)} = \{3, 5\}$, demonstrating that the bound is tight. □

B. Perfect polyphase sequences

A *polyphase sequence* is a sequence whose elements are all complex roots of unity of the form $exp(i2\pi x)$ where x is a rational number and $i = \sqrt{-1}$. Many studies have been done in the construction of perfect polyphase sequences. Mow [?] classified all known perfect polyphase sequences into four classes: generalized Frank sequences [?], generalized chirp-like sequences [?], Milewski sequences [?], and perfect polyphase sequences that associated with generalized bent functions [?]. Mow also proposed a unified construction of perfect polyphase sequences and conjectured that the unified construction describes all the perfect polyphase sequences that exist.

Generalized Frank sequences are perfect polyphase sequences which are from one-dimensional bent functions and were proposed by Kumar, Scholtz and Welch [?]. These sequences were first discovered by Frank and Zadoff [?] in the case of identity permutation. Heimiller [?] found the sequences $\omega_{N^2}^{N\cdot\pi(t_1)(t_2+h(t_1))}$ for the case of prime N, where h is also an arbitrary function on $\mathbb{Z}_N$. Generalized Frank sequences are a more general family, and are defined as follows.

Lemma 4. *[?] Let N be a positive integer and ω_N be a primitive N-th root of unity. Let*

(i) π be a permutation of elements in $\mathbb{Z}_N$ and let

(ii) σ be an arbitrary function from $\mathbb{Z}_N$ to $\mathbb{Z}_{N^2}$.

Then $s(t) = \omega_{N^2}^{N\cdot t_2\pi(t_1)+\sigma(t_1)}$ where $t = t_1 + t_2 \cdot N$, $0 \le t_1, t_2 < N$ is a perfect sequence of period N^2.

By Lemma ??, there are in total $N!N^{2N}$ perfect sequences of period N^2. In order to generate an optimal set from these sequences, the maximum cross-correlation magnitude of any two distinct sequences should be N. There exist many studies on perfect sequences with optimal cross-correlation (see Table ??). However, these constructions are trivial when N is even, which means no pair of perfect sequences of even period with optimal cross-correlation has been reported. In next section, we present a family of perfect sequences of period N^2 based on Lemma ??, whose maximum cross-correlation magnitude of any two distinct sequences is $2N$. The number of sequences in this family can be N when N is even.

III. Families of perfect sequences with low cross-correlation

In this section, we build a connection between generalised Frank sequences and Florentine arrays, which allows us to generate a family of perfect sequences with a large family size and low cross-correlation.

Let N be a positive integer. Let C be an $F(N) \times N$ Florentine array over $\mathbb{Z}_N$, where $F(N)$ is the maximum number such that an $F(N) \times N$ circular Florentine array exists. Let $\mathcal{A} = \{\beta_1, \beta_2, \ldots, \beta_{F(N)}\}$ be a set of permutations over $\mathbb{Z}_N$ from the rows of C. A set of sequences of period N^2 is defined as

$$\mathcal{S} = \{s_i \mid s_i(t) = \omega_{N^2}^{N\cdot\beta_i(t_1)t_2+\sigma(t_1)}, \beta_i \in \mathcal{A}\} \quad (1)$$

where $t = t_1 + t_2 \cdot N$, $0 \le t_1, t_2 < N$, and σ is an arbitrary function from $\mathbb{Z}_N$ to $\mathbb{Z}_{N^2}$.

Theorem 1. *The set $\mathcal{S}$ defined by (??) is a family of perfect sequences of size $F(N)$ with $R_c = 2N$.*

Proof. Since each $\beta_i \in \mathcal{A}$ is a permutation over $\mathbb{Z}_N$, each sequence in $\mathcal{S}$ is perfect by Lemma ??. For any shift $0 \le \tau < N^2$, we rewrite $\tau = \tau_1 + \tau_2 \cdot N$, where $0 \le \tau_1, \tau_2 < N$, and define

$$\delta_{t_1}^{\tau_1} = \begin{cases} 0, & \text{if } t_1 + \tau_1 < N, \\ 1, & \text{if } t_1 + \tau_1 \ge N. \end{cases}$$

TABLE III: Families of perfect polyphase sequences with low cross-correlation

References	[??]	[??][??]	[??][??]	[??]	[?]	[??]	[??]	[??]	[??]	[?]	[??][??]	this paper
Class of perfect sequences	Unified construction		Generalised chirp-like polyphase sequences			Generalised Frank sequences						
Period of perfect sequences	rm^2	rm^2 ($r \neq 1$)	N	rm^2	p^{2k+1}	Q^2	P^2	P^{2h}	P^2	N^2	N^2	N^2
The family size	$p-1$	$\min\{r^*-1, F_c(m)\}$	$p-1$	$p-1$	$p-1$	$\frac{p+1}{2}$	$p-1$	$p-1$	$p-1$	$p-1$	$F_c(N)$	$F(N)$

N, r, m and h are positive integers; P is an odd prime; Q is an odd integer; p is the smallest prime divisor of the period; r^* is the smallest prime divisor of r; $F_c(m)$ is the maximum number such that an $F_c(m) \times m$ circular Florentine array exists;
$F(N)$ is the maximum number such that an $F(N) \times N$ Florentine array exists;

Let $\mathbf{s}_i$ and $\mathbf{s}_j$ be two sequences in $\mathcal{S}$, where $1 \leq i \neq j \leq F(N)$. We rewrite $\tau = \tau_1 + \tau_2 \cdot N$, where $0 \leq \tau_1, \tau_2 < N$, and define

$$\delta_{t_1,\tau_1} = \begin{cases} 0 & \text{if } t_1 + \tau_1 < N, \\ 1 & \text{if } t_1 + \tau_1 \geq N. \end{cases}$$

The cross-correlation between $\mathbf{s}_i$ and $\mathbf{s}_j$ is given by

$$\begin{aligned} R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) &= \sum_{t=0}^{N^2-1} s_i(t+\tau) s_j^*(t) \\ &= \sum_{t_2=0}^{N-1}\sum_{t_1=0}^{N-1} \omega_{N^2}^{N\cdot\beta_i(t_1+\tau_1)(t_2+\tau_2+\delta_{t_1,\tau_1})+\sigma(t_1+\tau_1)} \cdot \omega_{N^2}^{-(N\cdot\beta_j(t_1)t_2+\sigma(t_1))} \\ &= \sum_{t_1=0}^{N-1} \omega_{N^2}^{N\cdot\beta_i(t_1+\tau_1)(\tau_2+\delta_{t_1,\tau_1})+\sigma(t_1+\tau_1)-\sigma(t_1)} \sum_{t_2=0}^{N-1} \omega_N^{(\beta_i(t_1+\tau_1)-\beta_j(t_1))t_2}. \end{aligned}$$

The inner sum of the last identity above is zero unless

$$\beta_i(t_1+\tau_1) \equiv \beta_j(t_1) \mod N.$$

Since β_i and β_j are two rows from a Florentine array, the above equation has at most two solutions in $\mathbb{Z}_N$ for $\forall \tau_1 \in \mathbb{Z}_N$ and $i \neq j$ by Lemma ??. Therefore, we have $|R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| \leq 2N$ for all $0 \leq \tau < N^2 - 1$ and $i \neq j$. □

Example 1. Let $N = 6$ and a 6×6 Florentine array is provided in Table ??. Let $\mathcal{A} = \{\beta_1, \beta_2, \ldots, \beta_6\}$ denote the set of permutations from the rows of the Florentine array. For simplicity, let $\sigma = 0$. Then a set of sequences of period 225 is defined as

$$\mathcal{S} = \{\mathbf{s}_i \mid s_i(t) = \omega_{36}^{\pi_i(t_1)t_2}, 1 \leq i \leq 6\},$$

where $t = t_1 + t_2 \cdot 6$, $0 \leq t_1, t_2 < 6$, $\pi_i \in \mathcal{A}$ for $1 \leq i \leq 6$. It is verifiable that

- *each sequence is a perfect sequence of period 36; and*
- *$|R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| \leq 12$ for any $0 \leq \tau < 6$, $1 \leq i \neq j \leq 6$.*

Therefore, the set $\mathcal{S}$ is a family of 6 perfect sequences of period 36 with $R_c = 12$, which are consistent with Theorem ??.

Given an $F(N) \times N$ Florentine array, we can get a family of $F(N)$ generalised Frank sequences of period N^2, where N is a positive integer and $F(N)$ is the maximum number such that an $F(N) \times N$ Florentine array exists. Table ?? gives a list of known results. Note that R_c in all the other works is equal to the square root of the period, which means optimal cross-correlation. However, the family size in the previous works is either determined by the smallest prime divisor of the period or the existence of circular Florentine arrays. The properties of Florentine arrays in Lemma ?? implies that the family size is larger in this paper. Furthermore, the number of rows in a Florentine array for even N, can be equal to N (see Table ??), which allows us to derive perfect sequences with low cross-correlation with family size N. In contrast, the family size in all the other works is equal to one when the period of the sequences is even.

IV. Conclusion

We derived a family of perfect sequences with low cross-correlation based on Florentine arrays. The number of the perfect sequences depends on the existence of Florentine arrays. The properties of Florentine arrays assure that the family size is larger than that in the previous works. The previous constructions are trivial when the period of the perfect sequences is even. In this work, a small compromise on the optimality of the cross-correlation allows us to derive an non-trivial construction of perfect sequences with low cross-correlation for even period.

Acknowledgment

This work was supported in part by Innlandet Fylkeskommune.