New Framework for Sequences With Perfect Autocorrelation and Optimal Crosscorrelation

Min Kyu Song, *Member, IEEE*, and Hong-Yeop Song, *Senior Member, IEEE*

***Abstract*— In this paper, we give a new framework for constructing perfect sequences, called generalized Milewski sequences, over various alphabets including Polyphase (PSK) as well as Amplitude-and-Polyphase (APSK) in general, and for constructing optimal sets of such perfect sequences by using combinatorial designs, called circular Florentine arrays. Specifically, we prove that, given any positive integer $m \geq 1$, (i) there exists a perfect sequence of period mN^2 for any positive integer N if there exists a perfect sequence (polyphase or not) of length m; (ii) an optimal k-set of perfect sequences of length mN^2 can be constructed if there exist both a $k \times N$ circular Florentine array and an optimal k-set of perfect sequences all of length m. This enables us to find some optimal k-set of perfect sequences where $k > p_{\min} - 1$, where $p_{\min}$ is the smallest prime factor of mN^2.**

***Index Terms*— Perfect sequences, perfect autocorrelation, optimal crosscorrelation, circular florentine arrays, polyphase, amplitude and polyphase (APSK), APSK+.**

I. Introduction

MODERN communication systems and radar systems use discrete time signals, which are defined over an alphabet of some complex numbers. Some famous examples of these alphabets with two-dimensional constellations are: Polyphase (PSK), PSK+, Amplitude-and-Polyphase (APSK), APSK+, etc. Herein, '+' symbol means an extended alphabet by allowing use of the value 'zero'. The discrete time signals are usually called sequences, and these are periodically repeated for special purposes: synchronization [1], channel estimation [28], direct-sequence code-division multiple access [5], [13], [17] in digital communication systems, ranging [2], [4], [26], and so forth. Those applications measure the similarity between the transmitted sequence and the received one by using matched filters to distinguish and/or to extract the desired information from the backgrounds. Herein, the measure of similarity is called autocorrelation when the (received) sequence is compared with cyclic-shifts of the same kind, and is called crosscorrelation when it is compared with cyclic-shifts of different kinds in the family. Therefore, to distinguish the desired sequence from others, it is most important to design a single sequence or a family of sequences with low autocorrelation and/or crosscorrelation magnitudes.

For the case of autocorrelation, it is obvious that zero magnitude for any non-zero time shift is the best. Such a sequence is called "perfect" and has been investigated over various constellations for several decades. The initial interest has been on binary perfect sequences of period N. It is now well-known that no example of binary perfect sequences of period $N > 4$ is known and it is conjectured that any binary sequence of period $N > 4$ does not achieve the zero autocorrelation magnitude [13], [17]. The next target is those over some various phase shift keying (PSK) constellations. Such perfect sequences are called perfect polyphase sequences or perfect root-of-unity sequences, and lots of constructions have been proposed [8], [10], [14], [19], [23], [28], [29], [31], [32], [34]. In [29], Mow categorized all the previously known perfect polyphase sequences into four classes: the generalized Frank sequences [23], the generalized chirp-like polyphase sequences [34], Milewski sequences [28], and the perfect sequences from the generalized bent functions due to Chung and Kumar [10]. He also gave some unified constructions of perfect polyphase sequences and proposed a fact that his last unified construction in [31] can generate all the (so-far) *known* perfect polyphase sequences and proposed a conjecture that there exists essentially *no new* example.

Meanwhile, perfect non-polyphase sequences have also been considered. Non-polyphase perfect sequences have been proposed over PSK+ constellations [6], [7], [20], [22] and over QAM (quadrature amplitude modulation) constellations [6], [46]. Recently, these works on perfect sequences over QAM constellation have been extended to the Gaussian integer sequences, since any conventional QAM (rectangular QAM) constellation can be represented by using Gaussian integers [21], [25], [33]. Obviously, when these perfect Gaussian integer sequences are real-valued, they become perfect sequences over ASK (amplitude shift keying) constellation.

On the other hand, using Sarwate's analysis on minimizing the maximum crosscorrelation magnitude of sets of perfect sequences [35], many researchers have proposed sets of perfect sequences with "optimal" crosscorrelation magnitude in terms of Sarwate's bound [3], [29], [32], [34], [44]. So far, these constructions for correlation-optimal sets of perfect sequences

Manuscript received January 11, 2019; revised October 14, 2020; accepted August 17, 2021. Date of publication August 24, 2021; date of current version October 20, 2021. This work was supported by the National Research Foundation of Korea (NRF) funded by the Korean Government through Ministry of Science, ICT and Future Planning (MSIP) under Grant 2017R1A2B4011191. An earlier version of this paper was presented in part at SETA 2018. *(Corresponding author: Hong-Yeop Song.)*

Min Kyu Song was with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, South Korea. He is now with Agency for Defence Development, Daejeon 34186, South Korea (e-mail: mksong@add.re.kr).

Hong-Yeop Song is with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, South Korea (e-mail: hysong@yonsei.ac.kr).

Communicated by K. Schmidt, Associate Editor for Sequences.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2021.3107611.

Digital Object Identifier 10.1109/TIT.2021.3107611

are known *only* over the polyphase constellations. These constructions are based on Frank sequences [3], [30], [44] or the generalized Frank sequences [32], [41], the generalized chirp-like polyphase sequences [34], and Mow's first unified construction [29].

Let $p_{\min}$ be the smallest prime factor of the period L of perfect sequences. Then the size of the previously known correlation-optimal sets of perfect sequences of period L cited above [29], [30], [32], [34], [44] can at most achieve $p_{\min} - 1$. One interesting point is that *no* example of a correlation-optimal set of size more than $p_{\min} - 1$ is known so far, and this number has not been shown to be an upper bound for any reason.

Constructing perfect sequences of longer period from those of shorter period may be a good approach over non-polyphase constellations [27], [33], [42]. The direct product construction [27] is the most well-known technique which produces perfect sequences of composite period pq from two perfect sequences of periods p and q, where p is coprime to q. Recently, the 'zero-padding and convolution' construction was introduced for generating perfect Gaussian integer sequences of longer period [33]. Some perfect sequences over Amplitude-and-Polyphase (APSK) alphabet have been proposed recently in [42].

In this paper, we give a new framework for constructing perfect sequences, called generalized Milewski sequences, a special case of which has been presented recently in [42], over various alphabets including Polyphase (PSK) as well as Amplitude-and-Polyphase (APSK) in general, and for constructing optimal sets of such perfect sequences by using combinatorial designs, called circular Florentine arrays. Specifically, we prove that, given any positive integer $m \geq 1$, (i) there exists a perfect sequence of period mN^2 for any positive integer N if there exists a perfect sequence (polyphase or not) of length m (Theorems 1 and 2); (ii) an optimal k-set of perfect sequences of length mN^2 can be constructed if there exist both a $k \times N$ circular Florentine array and an optimal k-set of perfect sequences all of length m (Theorems 3 and 4). This enables us to find some optimal k-set of perfect sequences where $k > p_{\min} - 1$, where $p_{\min}$ is the smallest prime factor of the length mN^2 of perfect sequences.

After some preliminaries in Section II, we present our main contribution of this paper in Section III. We first give our main framework, which is a special type of interleaved sequences. In Section III-A, we prove the necessary and sufficient condition for perfect autocorrelation of the output sequences from the main construction, which are called the generalized Milewski sequences. Section III-B is devoted to describing sets of generalized Milewski sequences which are optimal in terms of Sarwate's bound. The connection between optimal sets of generalized Milewski sequences and circular Florentine arrays is also given here. We also derive the maximum size of optimal sets of generalized Milewski sequences of length mN^2, which also describes the maximum size of optimal sets constructed by using all the known perfect polyphase sequences. Section IV concludes the paper with some concluding remarks.

II. Preliminaries

We will briefly review some notation and some well-known results which are useful in our presentation of the main result later.

- A k-set is a set of size k and an N-subset is a subset of size N.
- $\mathbb{Z}$ is the set of integers and $\mathbb{Z}_N$ is the integers modulo N.
- ω_N is a complex primitive N-th root of unity. Without subscript, we fix that ω is always a complex primitive mN-th root of unity for positive integers m and N.
- $\mathcal{U}_N$ is the set of all possible sequences of period N over the complex unit circle.
- A sequence $\boldsymbol{s}$ of length L is denoted by $\boldsymbol{s} = \{s(n)\}_{n=0}^{L-1}$. For an integer n with $0 \leq n < L$, $s(n)$ denotes the n-th term of $\boldsymbol{s}$. For n outside this range, $s(n)$ may denote the $n \pmod L$-th term of $\boldsymbol{s}$, where the sequence is considered to be repeating periodically with period L. Therefore, we may say a sequence of length L and that of period L interchangeably in general. However, a sequence of length L is sometimes used to denote a vector of finite length L in some formula. The distinction may be clear in the context. All the sequences in this paper are defined over the complex numbers.
- Given two sequences $\boldsymbol{s} = \{s(n)\}_{n=0}^{L-1}$ and $\boldsymbol{f} = \{f(n)\}_{n=0}^{L-1}$ both of period L, we may say the following:
  - $\boldsymbol{s} = \boldsymbol{f}$ if $s(n) = f(n)$ for all n;
  - $\boldsymbol{s}$ is a cyclic shift of $\boldsymbol{f}$ if there exists an integer τ such that $s(n) = f(n+\tau)$ for all n.
- The periodic (unnormalized) correlation between $\boldsymbol{s} = \{s(n)\}_{n=0}^{L-1}$ and $\boldsymbol{f} = \{f(n)\}_{n=0}^{L-1}$ both of period L at shift τ is denoted by $C_{\boldsymbol{s},\boldsymbol{f}}(\tau)$, and is defined by

$$C_{\boldsymbol{s},\boldsymbol{f}}(\tau) = \sum_{n=0}^{L-1} s(n+\tau) f^*(n),$$

  where $n+\tau$ is computed mod L and the asterisk refers to the complex conjugate. Note that it can be any complex number.
  - When $\boldsymbol{f}$ is a cyclic shift of $\boldsymbol{s}$, i.e., when they are cyclically equivalent, the above correlation becomes autocorrelation of $\boldsymbol{s}$, and is denoted by $C_{\boldsymbol{s}}(\tau)$. In this case, the energy allocated to the sequence $\boldsymbol{s}$ is given by $C_{\boldsymbol{s}}(0)$ and denoted by $E_{\boldsymbol{s}}$.
  - Otherwise, the above correlation $C_{\boldsymbol{s},\boldsymbol{f}}(\tau)$ is called crosscorrelation of $\boldsymbol{s}$ and $\boldsymbol{f}$.
- A sequence $\boldsymbol{s} = \{s(n)\}_{n=0}^{L-1}$ is called a *perfect sequence* if $C_{\boldsymbol{s}}(\tau) = 0$ for all $\tau \not\equiv 0 \pmod L$.
  - It is well-known that, $\{s(n)\omega_L^{an}\}_{n=0}^{L-1}$ is a perfect sequence of length L for any integer a, whenever $\boldsymbol{s}$ is a perfect sequence of length L [13].
  - In general, a perfect sequence $\boldsymbol{s}$ of length L is N-modulatable [44] for a divisor N of L if the sequence $\{s(n)\mu(n)\}_{n=0}^{L-1}$ is also perfect for any $\boldsymbol{\mu} \in \mathcal{U}_N$.

  - We note that some similar property is implied in the earlier work by Kumar, Scholtz, and Welch [23, Thm. 3].

- Let $\mathcal{H}$ be a set of perfect sequences of period L in which any sequence $\boldsymbol{s} \in \mathcal{H}$ has the same energy $E_{\boldsymbol{s}} = C_{\boldsymbol{s}}(0)$. Denote by θ_c the maximum crosscorrelation magnitude of sequences in the set $\mathcal{H}$. Then, Sarwate introduced a lower bound in 1979 as

$$\theta_c \geq \frac{E_{\boldsymbol{s}}}{\sqrt{L}}. \tag{1}$$

  Note that this bound does not depend on how many sequences the set $\mathcal{H}$ contains.
  - A pair of perfect sequences of period L is called an *optimal pair* if their crosscorrelation attains the lower bound in (1) with equality.
  - A set of perfect sequences of period L is called an *optimal set* if any pair of two distinct members in the set is an optimal pair.
  - The pair of perfect sequences $\boldsymbol{s}$ and $\boldsymbol{f}$ of length L and of energy E is optimal if and only if

$$|C_{\boldsymbol{s},\boldsymbol{f}}(\tau)| = \frac{E}{\sqrt{L}} \tag{2}$$

    for any τ [43].

- Let $\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{M-1}$ be M (not necessarily distinct) sequences all of length T, in which, for $0 \leq i \leq M-1$,

$$\boldsymbol{s}_i = \{s_i(n)\}_{n=0}^{T-1} = \{s_i(0), s_i(1), \ldots, s_i(T-1)\}.$$

  Then, the interleaved sequence $\boldsymbol{s}$ of period MT obtained from $\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{M-1}$ is denoted by

$$\boldsymbol{s} = \mathcal{I}(\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{M-1}) = \{s(n)\}_{n=0}^{MT-1}, \tag{3}$$

  whose n-th term is given by

$$s(n) = s_r(q)$$

  where q and r are the quotient and remainder when n is divided by M, i.e.,$n = qM + r$ with $0 \leq r < M$.
  - Note here that $(\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{M-1})$ in (3) is regarded as a $T \times M$ array, and the interleaving operator $\mathcal{I}$ reads row-by-row the $T \times M$ array to produce the sequence $\boldsymbol{s}$ of length MT.
  - Let

$$\boldsymbol{s} = \mathcal{I}(\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{M-1})$$

    and

$$\boldsymbol{f} = \mathcal{I}(\boldsymbol{f}_0, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_{M-1})$$

    be two interleaved sequences of length MT. Then, the correlation between $\boldsymbol{s}$ and $\boldsymbol{f}$ is given by

$$C_{\boldsymbol{s},\boldsymbol{f}}(\tau) = \sum_{r=M-r_\tau}^{M-1} \sum_{q=0}^{T-1} s_{r+r_\tau}(q+q_\tau+1) f_r^*(q) + \sum_{r=0}^{M-r_\tau-1} \sum_{q=0}^{T-1} s_{r+r_\tau}(q+q_\tau) f_r^*(q), \tag{4}$$

    where $\tau = q_\tau M + r_\tau$ with $0 \leq r_\tau < M$ [45].

- A $k \times N$ circular Florentine array [9], [11], [12], [16], [18], [36]–[40] is equivalent to a set of k distinct permutations $\pi_1, \pi_2, \ldots, \pi_k$ of the integers modulo N such that the equation

$$\pi_i(x+\tau) = \pi_j(x)$$

  has exactly one solution x for any two distinct permutations π_i and π_j and for any shift τ. We mention this here because it is closely related with the construction for an optimal set of generalized Milewski sequences.
  - Let $\mathcal{F}_c(N)$ denotes the largest integer such that an $\mathcal{F}_c(N) \times N$ circular Florentine array exists. The basic bound on $\mathcal{F}_c(N)$ is given by

$$p - 1 \leq \mathcal{F}_c(N) \leq N - 1,$$

    where p is the smallest prime factor of N.
  - It is well-known by [16] that if N is even, then

$$\mathcal{F}_c(N) = 1.$$

  - It is also well-known that if N is an odd prime, then $\mathcal{F}_c(N) = N - 1$, that is, an $(N-1) \times N$ circular Florentine array exists.
  - It is open (for more than 30 years) whether the existence of an $(N-1) \times N$ circular Florentine array implies that N is an odd prime.
  - It is interesting to find the current status of the lower bound on $\mathcal{F}_c(N)$ in [37] which is slightly better than the basic one $p-1$ for some small values of N.

III. Generalized Milewski (Polyphase/Non-Polyphase) Sequences

Following is a main framework of construction for sequences of longer period mN^2 by using sequences of shorter period m including the trivial case $m = 1$.

Definition 1 (Main Framework): Let m and N be two positive integers, ω be a complex primitive mN-th root of unity, $\mathcal{U}_N$ be the set of all possible sequences of length N over the complex unit circle. We define a family of interleaved sequences as

$$\mathcal{A}(B, \pi) = \{\mathcal{I}(\mathcal{S}(B, \pi, \boldsymbol{\mu})) \mid \boldsymbol{\mu} \in \mathcal{U}_N\}.$$

Herein, $\mathcal{S}(B, \pi, \boldsymbol{\mu})$ is the collection of sequences

$$\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{N-1},$$

which are defined as, for each $r = 0, 1, \ldots, N-1$,

$$\boldsymbol{s}_r = \left\{\beta_r(q)\mu(r)\omega^{q\pi(r)}\right\}_{q=0}^{mN-1}, \tag{5}$$

where

- B is a collection of N (not necessarily distinct) sequences $\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}$ all of length m,
- π is a function from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$.

The r-th column sequence $\boldsymbol{s}_r$ of length mN in (5) is shown in Fig. 1. Herein, each component sequence $\boldsymbol{\beta}_r = \{\beta_r(q)\}_{q=0}^{m-1}$ is repeated N times and the result is multiplied by $\mu(r)\omega^{q\pi(r)}$ for $q = 0, 1, \ldots, mN-1$. We would like to emphasize two special cases of the above framework of construction:

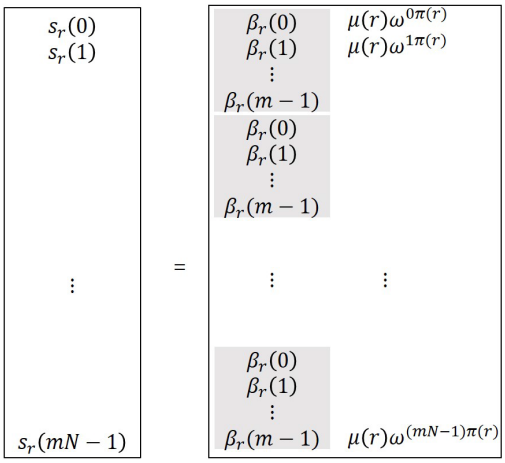


Fig. 1. The r-th column sequence $\boldsymbol{s}_r$ of the set $\mathcal{S}(B,\pi,\boldsymbol{\mu})$.

- We may write $\mathcal{A}(\boldsymbol{\beta},\pi)$ when
$$\boldsymbol{\beta}_0=\boldsymbol{\beta}_1=\cdots=\boldsymbol{\beta}_{N-1}=\boldsymbol{\beta}.$$
- When $\boldsymbol{\beta}=\{1\}$ in addition, we may write $\mathcal{A}(\{1\},\pi)$ and the length will be N^2.

We will investigate in the remaining of this paper when the members of $\mathcal{A}(B,\pi)$ are perfect sequences, and when any two members, one from $\mathcal{A}(B_1,\pi)$ and the other from $\mathcal{A}(B_2,\sigma)$, have optimal crosscorrelation. For this, the following plays some important role:

Definition 2: Let π and σ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$. We define
$$\Psi_{\pi,\sigma}(\tau)=\{x\in\mathbb{Z}_N \mid \pi(x+\tau)\equiv\sigma(x) \pmod N\}.$$
When $\pi=\sigma$, we use $\Psi_\pi(\tau)$ simply.

Let $B_1=\{\boldsymbol{\beta}_0,\boldsymbol{\beta}_1,\ldots,\boldsymbol{\beta}_{N-1}\}$, $B_2=\{\boldsymbol{\gamma}_0,\boldsymbol{\gamma}_1,\ldots,\boldsymbol{\gamma}_{N-1}\}$, and π,σ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$, and $\boldsymbol{\mu},\boldsymbol{\nu}$ be two members of $\mathcal{U}_N$. By (4), the correlation of $\boldsymbol{s}=\mathcal{I}(\mathcal{S}(B_1,\pi,\boldsymbol{\mu}))$ and $\boldsymbol{f}=\mathcal{I}(\mathcal{S}(B_2,\sigma,\boldsymbol{\nu}))$ is
$$C_{\boldsymbol{s},\boldsymbol{f}}(\tau)=\sum_{r=0}^{N-r_\tau-1}\sum_{q=0}^{mN-1}s_{r+r_\tau}(q+q_\tau)f_r^*(q)+\sum_{r=N-r_\tau}^{N-1}\sum_{q=0}^{mN-1}s_{r+r_\tau}(q+q_\tau+1)f_r^*(q),$$
where $\tau=q_\tau N+r_\tau$ with $0\le r_\tau<N$. By writing $q=um+t$ with $0\le t<m$, the first term of the RHS above becomes
$$\begin{aligned}&\sum_{r=0}^{N-r_\tau-1}\sum_{q=0}^{mN-1}s_{r+r_\tau}(q+q_\tau)f_r^*(q)\\&=\sum_{r=0}^{N-r_\tau-1}\mu(r+r_\tau)\nu^*(r)\omega^{\pi(r+r_\tau)q_\tau}\\&\quad\times\sum_{q=0}^{mN-1}\beta_{r+r_\tau}(q+q_\tau)\gamma_r^*(q)\omega^{[\pi(r+r_\tau)-\sigma(r)]q}\\&=\sum_{r=0}^{N-r_\tau-1}\mu(r+r_\tau)\nu^*(r)\omega^{\pi(r+r_\tau)q_\tau}\\&\quad\times\sum_{u=0}^{N-1}\omega_N^{[\pi(r+r_\tau)-\sigma(r)]u}\\&\quad\times\sum_{t=0}^{m-1}\beta_{r+r_\tau}(t+q_\tau)\gamma_r^*(t)\omega^{[\pi(r+r_\tau)-\sigma(r)]t}.\end{aligned}$$
By the similar way, the second term becomes
$$\begin{aligned}&\sum_{r=N-r_\tau}^{N-1}\sum_{q=0}^{mN-1}s_{r+r_\tau}(q+q_\tau+1)\ f_r^*(q)\\&=\sum_{r=N-r_\tau}^{N-1}\mu(r+r_\tau)\nu^*(r)\omega^{\pi(r+r_\tau)(q_\tau+1)}\\&\quad\times\sum_{u=0}^{N-1}\omega_N^{[\pi(r+r_\tau)-\sigma(r)]u}\\&\quad\times\sum_{t=0}^{m-1}\beta_{r+r_\tau}(t+q_\tau+1)\gamma_r^*(t)\omega^{[\pi(r+r_\tau)-\sigma(r)]t}.\end{aligned}$$
Herein, we use the following basic lemma:

Lemma 1: Let N be a positive integer. Then, for an integer a,
$$\sum_{u=0}^{N-1}\omega_N^{au}=\begin{cases}N, & \text{if } a\equiv 0 \pmod N,\\ 0, & \text{otherwise.}\end{cases}$$
By the lemma, it is easy to see that
$$\sum_{u=0}^{N-1}\omega_N^{[\pi(r+r_\tau)-\sigma(r)]u}=\begin{cases}N, & r\in\Psi_{\pi,\sigma}(r_\tau),\\ 0, & r\notin\Psi_{\pi,\sigma}(r_\tau).\end{cases}$$
Therefore, we finally get the following formula:

Lemma 2: For given $B_1=\{\boldsymbol{\beta}_0,\boldsymbol{\beta}_1,\ldots,\boldsymbol{\beta}_{N-1}\}$ and $B_2=\{\boldsymbol{\gamma}_0,\boldsymbol{\gamma}_1,\ldots,\boldsymbol{\gamma}_{N-1}\}$, let $\boldsymbol{s}=\mathcal{I}(\mathcal{S}(B_1,\pi,\boldsymbol{\mu}))$ and $\boldsymbol{f}=\mathcal{I}(\mathcal{S}(B_2,\sigma,\boldsymbol{\nu}))$ be two sequences of length mN^2 constructed by Definition 1. Then, the correlation between $\boldsymbol{s}$ and $\boldsymbol{f}$ at shift τ is, for $\tau=q_\tau N+r_\tau$ with $0\le r_\tau<N$,
$$\begin{aligned}&C_{\boldsymbol{s},\boldsymbol{f}}(\tau)\\&=N\sum_{r\in\Psi_{\pi,\sigma}(r_\tau)}\mu(r+r_\tau)\nu^*(r)\omega^{\pi(r+r_\tau)(q_\tau+\delta)}\\&\quad\times\left(\sum_{t=0}^{m-1}\beta_{r+r_\tau}(t+q_\tau+\delta)\gamma_r^*(t)\omega_m^{[\pi(r+r_\tau)-\sigma(r)]t}\right)\end{aligned}\quad(6)$$
where
$$\delta=\begin{cases}0, & \text{if } 0\le r<N-r_\tau,\\ 1, & \text{if } N-r_\tau\le r<N.\end{cases}$$

A. Condition for Perfect Autocorrelation

Theorem 1: Assume all the notations in Definitions 1, 2 and Lemma 2. Then, any sequence in $\mathcal{A}(B,\pi)$ is perfect if and only if the following conditions are satisfied:

1) $|\Psi_\pi(r_\tau)|=0$ for $r_\tau=1,2,\ldots,N-1$, that is, $\pi(x) \pmod N$ for $x=0,1,\ldots,N-1$ is a permutation over $\mathbb{Z}_N$.
2) B is a collection of perfect sequences all of period m with the same energy.

Proof: We will prove the sufficiency first. We begin by (6) with $\boldsymbol{s} = \boldsymbol{f} = \mathcal{I}(\mathcal{S}(B, \pi, \boldsymbol{\mu}))$. Now, it is enough to observe the following two cases: (i) $\tau \neq 0 \pmod N$ and (ii) $\tau = 0 \pmod N$ but $\tau \neq 0 \pmod{mN^2}$. We will write $\tau = q_\tau N + r_\tau$ with $0 \leq r_\tau < N$.

CASE(i) Assume that $0 < r_\tau < N$. Since π is a permutation over $\mathbb{Z}_N$, the set $\Psi_\pi(r_\tau)$ is empty for all $r_\tau = 1, 2, \ldots, N-1$. Therefore, (6) implies $C_{\boldsymbol{s}}(\tau) = 0$.

CASE(ii) Assume that $r_\tau = 0$, i.e., $\tau = q_\tau N$. Then, $\delta = 0$ for all r, and

$$\Psi_\pi(r_\tau = 0) = \{0, 1, 2, \ldots, N-1\}.$$

Therefore, (6) becomes

$$\begin{aligned} C_{\boldsymbol{s}}(q_\tau N) &= N \sum_{r \in \Psi_\pi(0)} \mu(r)\mu^*(r)\omega^{\pi(r)q_\tau} \\ &\quad \times \left(\sum_{t=0}^{m-1} \beta_r(t+q_\tau)\beta_r^*(t) \right) \\ &= N \sum_{r=0}^{N-1} \omega^{\pi(r)q_\tau} C_{\boldsymbol{\beta}_r}(q_\tau). \end{aligned} \tag{7}$$

When $q_\tau \not\equiv 0 \pmod m$, the value $C_{\boldsymbol{\beta}_r}(q_\tau) = 0$ for any $r = 0, 1, \ldots, N-1$ since they all are perfect sequences, and hence, $C_{\boldsymbol{s}}(\tau) = 0$. Otherwise, we let $q_\tau = ml$ for some integer l. Then, $C_{\boldsymbol{\beta}_r}(q_\tau) = C_{\boldsymbol{\beta}_r}(ml) = E_B$ for any $r = 0, 1, \ldots, N-1$ since they all have the same energy, say, E_B. Since $\pi(r) \pmod N$ is a permutation over $\mathbb{Z}_N$, we have

$$C_{\boldsymbol{s}}(mlN) = NE_B \sum_{r=0}^{N-1} \omega^{\pi(r)ml} = 0,$$

by Lemma 1 since $l \neq 0 \pmod N$.

We now will prove that the two conditions are satisfied necessarily if $\boldsymbol{s} = \mathcal{I}(\mathcal{S}(B, \pi, \boldsymbol{\mu}))$ is a perfect sequence of period mN^2 and with the energy $E_{\boldsymbol{s}} > 0$ for any $\boldsymbol{\mu} \in \mathcal{U}_N$. We write $\tau = q_\tau N + r_\tau$ with $0 \leq r_\tau < N$ and consider the cases where $r_\tau = 0$, i.e., $\tau = q_\tau N$. Then, using the expression for $C_{\boldsymbol{s}}(q_\tau N)$ as given in (7) and from the assumption that $\boldsymbol{s}$ is perfect, we have

$$\begin{aligned} C_{\boldsymbol{s}}(q_\tau N) &= N \sum_{r=0}^{N-1} \omega^{\pi(r)q_\tau} C_{\boldsymbol{\beta}_r}(q_\tau) \\ &= \begin{cases} E_{\boldsymbol{s}} & \text{if } \ q_\tau N = 0 \pmod{mN^2}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{8}$$

Write $q_\tau = gm + h$ with $0 \leq h < m$. Then, by considering all the cases of $h = 0$, we have, for $q_\tau = 0, m, 2m, \ldots, (N-1)m$ which are all $0 \bmod m$, the relation (8) becomes

$$N[\omega_N^{g\pi(r)}] \begin{bmatrix} C_{\boldsymbol{\beta}_0}(0) \\ C_{\boldsymbol{\beta}_1}(0) \\ \vdots \\ C_{\boldsymbol{\beta}_{N-1}}(0) \end{bmatrix} = E_{\boldsymbol{s}} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{9}$$

where $g, r = 0, 1, \ldots, N-1$ are row and column indices of the matrix $[\omega_N^{g\pi(r)}]$, respectively. Multiply the (unnormalized) Fourier matrix of order N of the following form $[\omega_N^{gr}]$ to both LHS and RHS of (9). Then, we have

$$N[\,\omega_N^{gr}\,][\omega_N^{g\pi(r)}] \begin{bmatrix} C_{\boldsymbol{\beta}_0}(0) \\ C_{\boldsymbol{\beta}_1}(0) \\ \vdots \\ C_{\boldsymbol{\beta}_{N-1}}(0) \end{bmatrix} = E_{\boldsymbol{s}} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}. \tag{10}$$

Now, two matrices of order N on LHS of the above are the (unnormalized) Fourier matrix and its column-changed version by π where the r-th column comes to the $\pi(r) \pmod N$-th column for each $r = 0, 1, \ldots, N-1$. Now, if $\pi(x) \pmod N$ is not a permutation of $\mathbb{Z}_N$, then, there must be at least one all-zero row in the product of two matrices $[\omega_N^{gr}][\omega_N^{g\pi(r)}]$, which gives the value zero on LHS of (10). This is a contradiction since (10) also shows that it is non-zero on RHS. Therefore, $\pi(x) \pmod N$ must be a permutation of $\mathbb{Z}_N$.

Now, assume that $\pi(x) \pmod N$ is a permutation over $\mathbb{Z}_N$. Then, the matrix $[\omega_N^{g\pi(r)}]$ in (9) is a Vandermonde matrix of full rank. By solving (9), we have

$$C_{\boldsymbol{\beta}_0}(0) = C_{\boldsymbol{\beta}_1}(0) = \cdots = C_{\boldsymbol{\beta}_{N-1}}(0) = \frac{E_s}{N^2},$$

that is all the $\boldsymbol{\beta}_i$'s are the same energy.

Similarly, for each $h = 1, 2, \ldots, m-1$, we have, from (8),

$$\left[\omega^{(gm+h)\pi(r)}\right] \begin{bmatrix} C_{\boldsymbol{\beta}_0}(h) \\ C_{\boldsymbol{\beta}_1}(h) \\ \vdots \\ C_{\boldsymbol{\beta}_{N-1}}(h) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

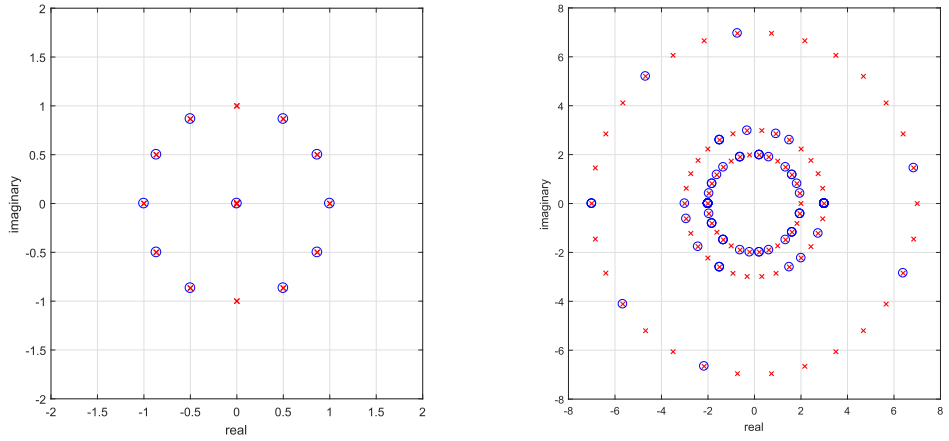
where the coefficient matrix $[\omega^{(gm+h)\pi(r)}]$ is a Vandermonde matrix of full rank, where $g, r = 0, 1, \ldots, N-1$ are row and column indices. Therefore, we conclude that $\boldsymbol{\beta}_r$ is perfect for any r. ∎

Remark 1: The main framework in Definition 1 has been motivated by Milewski's perfect polyphase sequence construction. Gabidulin also considered similar one independently [15, Theorem 2], but it is essentially a subset of Milewski sequences [13].

The main framework in Definition 1 with the necessary and sufficient condition for perfect autocorrelation in Theorem 1 is therefore a generalization into (i) those perfect sequences over polyphase and/or non-polyphase alphabets and (ii) those prefect sequences with more choices on period. In the remaining of this paper, therefore, any sequence constructed by the main construction will be called *a generalized Milewski sequence* when it has the perfect autocorrelation. If, furthermore, it is a polyphase sequence, then it will be called *a generalized Milewski polyphase sequence*.

Example 1: The generalized Milewski sequences from Theorem 1 could be either polyphase or non-polyphase (APSK when non-polyphase). Herein, we give some examples when the generalized Milewski sequences are over the APSK constellations. For the simplicity, we let π be the identity function and $\boldsymbol{\mu}$ be the all-one sequence.

1) By using $\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \{0, -1, 1, 0, 1, 1\}$ given by [24], we have a generalized Milewski sequence of length 24



(a) PSK+ constellation

(b) APSK constellation

Fig. 2. Constellations of perfect sequences in Example 1.

(when $N = 2$ and $m = 6$) over the constellation shown in Fig. 2-(a). The constellation has 13 different symbols with mark '$\times$'. Among them, only 11 symbols with mark '$\circ$' are essentially used.

2) By using

$$\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \boldsymbol{\beta}_2 = \{3, -2, 3, -2, -2, 3, -2, -7, -2, -2\}$$

given by [21], we have a generalized Milewski sequence of length 90 (when $N = 3$ and $m = 10$) over the constellation shown in Fig. 2-(b).

We would also remark that the generalized Milewski sequences are N-modulatable in the sense of [44] or the discussion in Section II. This is true even when the generalized Milewski sequences are non-polyphase perfect sequences.

For a composite number N, let N_1 be a proper divisor of N and B be a collection of N perfect sequences of length m and the same energy. Then, it is possible to construct a generalized Milewski sequence $\boldsymbol{s}$ of length mN^2 in two different ways:

- **(Direct method):** $\boldsymbol{s}$ is constructed by using B directly.
- **(Two-step method):** $\boldsymbol{s}$ is constructed by using a collection of generalized Milewski sequences of period mN_1^2, each of which is constructed by using only some N_1 perfect sequences of B.

Theorem 2: Assume that N is a composite number.

1) Any generalized Milewski sequence of length mN^2 from the two-step method can be also obtained by the direct method.
2) There exists a generalized Milewski sequence of length mN^2 from the direct method which cannot be obtained by the two-step method.

Proof: See Appendix. ∎

Remark 2: The generalized Milewski polyphase sequences from the main construction by using Zadoff-Chu sequences become the perfect polyphase sequences constructed by Mow [31]. This can be simply shown by letting m be a square-free integer, N be any positive integer, and $B = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}\}$ be a collection of (not necessarily all distinct) Zadoff-Chu sequences [8] of period m.

The perfect polyphase sequences constructed by Mow is known to contain all the known perfect polyphase sequences so far, and it is conjectured that there is no new perfect polyphase sequences [31]. The conjecture still remains open, since you will obtain no new perfect polyphase sequence from the main construction whichever collection of Mow's perfect polyphase sequences you might use. The generalized Milewski polyphase sequences by using any of Mow's sequences is a result of two-step method since any of Mow's sequences is a result of the main construction. See Theorem 2.

Remark 3: For any given function π from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$, write $\pi(x)$ as

$$\pi(x) = q_\pi(x)N + r_\pi(x) \tag{11}$$

with $0 \le r_\pi(x) < N$. The proof (i) above implies that q_π has nothing to do with the perfectness of the generalized Milewski sequences. On the other hand, q_π is related with the alphabet size of the resulting sequences.

For a given permutation r_π over $\mathbb{Z}_N$, let

$$q_\pi(x) = -r_\pi(x)N^{-1} \pmod{m/g}, \tag{12}$$

where $g = \gcd(m, N)$. Then, $\pi(x)$ becomes a multiple of m/g for all x, and hence the term $\omega^{q\pi(x)}$ in (5) is essentially gN-root of unity. Therefore, when π in (11) satisfies (12), the alphabet size could be determined easily even when the input sequeces $\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}$ are not polyphase. As shown in Table I, the generalized Milewski construction generates perfect PSK+ sequences which is more flexible on the choice of length and alphabet size.

The generalized Milewski construction can also be applied to perfect Gaussian integer sequences by the similar way, but, to maintain the result being over gaussian integers, there is a strong restriction: N can be either 2 or 4 and gN should be less than or equal to 4.

We finish this subsection by giving a formula for calculating energy efficiency of the generalized Milewski sequences. Here, the energy efficiency $\eta_{\boldsymbol{s}}$ of a given sequence $\boldsymbol{s}$ of period L with energy $E_{\boldsymbol{s}}$ is defined by [13]

$$\eta_{\boldsymbol{s}} = \frac{\sum_{n=0}^{L-1} |s(n)|^2 / L}{\max\limits_{0 \le n < L} |s(n)|^2} = \frac{E_{\boldsymbol{s}}/L}{\max\limits_{0 \le n < L} |s(n)|^2}.$$

Corollary 1: Let $\boldsymbol{s} \in \mathcal{A}(B, \pi)$ be a generalized Milewski sequence from the collection B in which all the sequences

TABLE I
COMPARISON WITH SOME PERFECT SEQUENCES OVER PSK+ CONTELLATION

Construction		period(L)	Alphabet	note
Previous results	Ipatov [22]	$L=\frac{q^n-1}{q-1}$	BPSK+ (Ternary)	$q=p^s$ for $s\geq 1$
	Høholdt [20]	$L=\frac{q^{2n+1}-1}{q-1}$	BPSK+ (Ternary)	$q=2^s$ for $s\geq 1$
	Boztaş [6]	$L=\frac{q^n-1}{q-1}$	$(q-1)$-PSK+	$q=p^s$ for $s\geq 1$
	Boztaş [7]	$L=\frac{q^n-1}{q-1}$	n-PSK+	$q=p^s$ for $s\geq 1$
This paper	By using Ipatov seq.	$L=mN^2=\frac{q^n-1}{q-1}N^2$	(gN)-PSK+	$N\geq 2$ and $g=\gcd(m,N)$
	By using Høholdt seq.	$L=mN^2=\frac{q^{2n+1}-1}{q-1}N^2$	(gN)-PSK+	$N\geq 2$ and $g=\gcd(m,N)$

have the same energy E_B. Denote by η_r the energy efficiency of the r-th sequence $\boldsymbol{\beta}_r$ in B. Then, $\eta_{\boldsymbol{s}} = \min\{\eta_0,\eta_1,\ldots,\eta_{N-1}\}$.

Proof: It is enough to observe that

$$E_{\boldsymbol{s}}/L = E_B N^2/mN^2 = E_B/m,$$

and

$$\max_{0\leq n<mN^2}|s(n)|^2 = \max_{\substack{0\leq r<N,\\ 0\leq q<mN}}|\beta_r(q)|^2.$$

■

B. Conditions for Optimal Crosscorrelation

To describe optimal crosscorrelation of generalized Milewski sequences, the following lemma is useful:

Lemma 3 ([41]): Let π and σ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$, and both are permutations over $\mathbb{Z}_N$ when the range is reduced to $\mathbb{Z}_N$. Recall the definition of $\Psi_{\pi,\sigma}(\tau)$ in Definition 2. Then, we have

$$\sum_{\tau=0}^{N-1}|\Psi_{\pi,\sigma}(\tau)| = N. \tag{13}$$

Theorem 3: Let $B_1 = \{\boldsymbol{\beta}_0,\boldsymbol{\beta}_1,\ldots,\boldsymbol{\beta}_{N-1}\}$ and $B_2 = \{\boldsymbol{\gamma}_0,\boldsymbol{\gamma}_1,\ldots,\boldsymbol{\gamma}_{N-1}\}$ be two collections of perfect sequences all of length m and the same energy E_B. Construct generalized Milewski sequences $\boldsymbol{s}\in\mathcal{A}(B_1,\pi)$ and $\boldsymbol{f}\in\mathcal{A}(B_2,\sigma)$ with the same energy $E_{\boldsymbol{s}} = E_B N^2$ from Theorem 1. Then, $\boldsymbol{s}$ and $\boldsymbol{f}$ have optimal crosscorrelation if and only if the following conditions are satisfied for each $r_\tau = 0,1,\ldots,N-1$:

1) $\Psi_{\pi,\sigma}(r_\tau)=\{x\}$, i.e., $|\Psi_{\pi,\sigma}(r_\tau)|=1$; and
2) for the unique $x\in\Psi_{\pi,\sigma}(r_\tau)$, the pair of sequences

$$\left\{\beta_{x+r_\tau}(t)\,\omega_m^{\pi(x+r_\tau)t}\right\}_{t=0}^{m-1} \quad\text{and}\quad \left\{\gamma_x(t)\,\omega_m^{\sigma(x)t}\right\}_{t=0}^{m-1}$$

is optimal.

Proof: To prove the necessity, let $\boldsymbol{s} = \mathcal{I}(\mathcal{S}(B_1,\pi,\boldsymbol{\mu}))$ and $\boldsymbol{f} = \mathcal{I}(\mathcal{S}(B_2,\sigma,\boldsymbol{\nu}))$ for some $\boldsymbol{\mu},\boldsymbol{\nu}\in\mathcal{U}_N$, and assume that the pair of sequences $\boldsymbol{s}$ and $\boldsymbol{f}$ is optimal. Suppose on the contrary that

$$|\Psi_{\pi,\sigma}(r_\tau)|\geq 2$$

for some $\tau = q_\tau N + r_\tau$. Then, from Lemma 3, we can always find an integer τ' with $0\leq r_{\tau'}\leq N-1$ such that

$$|\Psi_{\pi,\sigma}(r_{\tau'})| = 0.$$

Then, $C_{\boldsymbol{s},\boldsymbol{f}}(\tau') = 0$ from (6), which is a contradiction to (2). Therefore, we conclude that $|\Psi_{\pi,\sigma}(r_\tau)| = 1$ for any $\tau = q_\tau N + r_\tau$.

Now, let x be the unique member of $\Psi_{\pi,\sigma}(r_\tau)$. Then, by Lemma 2, the crosscorrelation magnitude $|C_{\boldsymbol{s},\boldsymbol{f}}(\tau)|$ of $\boldsymbol{s}$ and $\boldsymbol{f}$ at shift $\tau = q_\tau N + r_\tau$ becomes

$$N\left|\sum_{t=0}^{m-1}\beta_{x+r_\tau}(t+q_\tau+\delta)\gamma_x^*(t)\omega_m^{[\pi(x+r_\tau)-\sigma(x)]t}\right|. \tag{14}$$

Since $\boldsymbol{s}$ and $\boldsymbol{f}$ form an optimal pair, by (2), we have

$$|C_{\boldsymbol{s},\boldsymbol{f}}(\tau)| = \frac{E_{\boldsymbol{s}}}{\sqrt{mN^2}} = \frac{E_B N}{\sqrt{m}},$$

and hence, we get the conclusion.

The sufficiency is easily shown by just calculating their crosscorrelation with the formula given in Lemma 2. It becomes obvious by considering (14). ■

Following is an interesting special case of the necessary and sufficient condition in Theorem 3 when the ranges of π and σ are the same N-subsets of $\mathbb{Z}_{mN}$:

$$\{\pi(x)\mid x\in\mathbb{Z}_N\} = \{\sigma(x)\mid x\in\mathbb{Z}_N\}. \tag{15}$$

Corollary 2: Let $\boldsymbol{s}\in\mathcal{A}(B_1,\pi)$ and $\boldsymbol{f}\in\mathcal{A}(B_2,\sigma)$ be two generalized Milewski sequences of period mN^2 with the same energy, in Theorem 3. Assume that two functions π and σ have the same range as in (15). Then, $\boldsymbol{s}$ and $\boldsymbol{f}$ have the optimal crosscorrelation if and only if the following conditions are satisfied for each $r_\tau = 0,1,\ldots,N-1$:

1) $\Psi_{\pi,\sigma}(r_\tau)=\{x\}$, i.e., $|\Psi_{\pi,\sigma}(r_\tau)|=1$; and
2) for the unique $x\in\Psi_{\pi,\sigma}(r_\tau)$, the pair of sequences $\boldsymbol{\beta}_{x+r_\tau}$ and $\boldsymbol{\gamma}_x$ is optimal.

Proof: Recall the decomposition of π in (11). We do the same for σ and write

$$\sigma(x) = q_\sigma(x)N + r_\sigma(x),$$

with $0\leq r_\sigma(x)<N$ for any $x\in\mathbb{Z}_N$.

By the assumption that the ranges of both π and σ are the same N-subsets of $\mathbb{Z}_{mN}$, and their reduction modulo N is a permutation over $\mathbb{Z}_N$ we have the following:

$$\pi(x+r_\tau) = \sigma(x) \pmod{mN}$$

whenever

$$\pi(x+r_\tau) = \sigma(x) \pmod{N}.$$

This implies that for $x\in\Psi_{\pi,\sigma}(r_\tau)$ the value $\pi(x+r_\tau)-\sigma(x)$ is a multiple of mN. ■

Corollary 2 implies that an optimal k-set of generalized Milewski sequences can be constructed if there exist both (1) at least one optimal k-set of perfect sequences all of period m with the same energy and (2) a k-set of functions

$\Pi = \{\pi_0, \pi_1, \ldots, \pi_{k-1}\}$ each of which is a function from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$ satisfying the following two properties: (i) for each i, the values $\pi_i(x) \pmod N$ for $x = 0, 1, \ldots, N-1$ are all distinct; and (ii) for any two distinct $\pi_i, \pi_j \in \Pi$,

$$\left|\Psi_{\pi_i,\pi_j}(r_\tau)\right| = 1,$$

for each $r_\tau = 0, 1, 2, \ldots, N-1$.

Note that the k-set of functions $\Pi = \{\pi_0, \pi_1, \ldots, \pi_{k-1}\}$ above with two properties is equivalent to a circular Florentine array of size $k \times N$ described at the end of Section II. With an abuse of language, we just call such a set of functions a circular Florentine array.

We first consider the simple case of using a trivial perfect sequence $\{1\}$ of length $m = 1$. Note that this sequence and itself can be regarded as a (trivial) optimal pair of perfect sequences of length 1. Then we can construct a k-set of optimal sequences of length N^2 whenever there exists a $k \times N$ circular Florentine array $\Pi = \{\pi_0, \pi_1, \ldots, \pi_{k-1}\}$ where each π_i is a permutation of $\mathbb{Z}_N$. Two examples of this case where $N = 15$ and $N = 27$ are shown in Example 2 below.

Example 2: Let $m = 1$ and $\boldsymbol{\mu}$ be the all-one sequence of length N. And, consider the trivial perfect sequence $\{1\}$.

1) For $N = 15$, the author of [37] gave an example of a circular Florentine array of size 4×15. By regarding each row of it as a permutation, we have

$$\begin{aligned}
\pi_0 &= (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14),\\
\pi_1 &= (0, 7, 1, 8, 2, 12, 3, 11, 9, 4, 13, 5, 14, 6, 10),\\
\pi_2 &= (0, 4, 11, 7, 10, 1, 13, 9, 5, 8, 3, 6, 2, 14, 12),\\
\pi_3 &= (0, 13, 7, 2, 11, 6, 14, 10, 3, 5, 12, 9, 1, 4, 8),
\end{aligned}$$

   where $\pi_i = (a_0, a_1, \ldots)$ denotes $\pi_i(j) = a_j$ for all i, j. Based on these four permutations, we obtain an optimal set of four perfect polyphase sequences of period $15^2 = 225$ by picking up a single perfect sequence from each and every $\mathcal{A}(\{1\}, \pi_0)$, $\mathcal{A}(\{1\}, \pi_1)$, $\mathcal{A}(\{1\}, \pi_2)$, $\mathcal{A}(\{1\}, \pi_3)$.
2) Using a 4×27 circular Florentine array in [37], one can similarly construct an optimal set of 4 perfect sequences of period $27^2 = 729$.

Remark 4: Until now, polyphase is the only constellation over which optimal sets have been constructed [30], [32], [34], [41], [43], [44]. Herein, any known optimal perfect polyphase sequence sets of period L is of size $p_{\min} - 1$, where $p_{\min}$ is the smallest prime factor of the period L. We would like to emphasize that the optimal sets given in Example 2 are the first example of optimal sets which are of size larger than $p_{\min} - 1$.

For $m > 1$, we need at least one k-set of optimal sequences of length m in addition to a $k \times N$ circular Florentine array in order to construct a k-set of optimal sequences of length mN^2. Consider simply the case of $k = 2$ here, and assume that we have both (1) a pair of optimal sequences $\{\boldsymbol{\beta}, \boldsymbol{\gamma}\}$ of length m and the same energy E_B and (2) a $2 \times N$ circular Florentine array $\Pi = \{\pi, \sigma\}$. Assume that π and σ have the same range so that Corollary 2 can be applied. We describe two different procedures of constructing a pair of sequences $\boldsymbol{s} \in \mathcal{A}(B_1, \pi)$ and $\boldsymbol{f} \in \mathcal{A}(B_2, \sigma)$ of length mN^2, where the difference is the choice of B_1 and B_2 using the pair $\{\boldsymbol{\beta}, \boldsymbol{\gamma}\}$.

- (Simple and Constant Assignment). We let B_1 have only $\boldsymbol{\beta}$ and B_2 have only $\boldsymbol{\gamma}$. That is, we use $\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \cdots = \boldsymbol{\beta}_{N-1} = \boldsymbol{\beta}$ and $\boldsymbol{\gamma}_0 = \boldsymbol{\gamma}_1 = \cdots = \boldsymbol{\gamma}_{N-1} = \boldsymbol{\gamma}$. Therefore, according to the notation in Remark 1, we have $\boldsymbol{s} \in \mathcal{A}(\boldsymbol{\beta}, \pi)$ and $\boldsymbol{f} \in \mathcal{A}(\boldsymbol{\gamma}, \sigma)$. Note that in this case we do not care for the sets $\Psi_{\pi,\sigma}(r_\tau)$ at all for $r_\tau = 0, 1, 2, \ldots, N-1$.
- (Other Assignment). We first have to determine the unique value $x \in \Psi_{\pi,\sigma}(r_\tau)$ for each $r_\tau = 0, 1, 2, \ldots, N-1$. This gives N pairs $(\boldsymbol{\beta}_{x+r_\tau}, \boldsymbol{\gamma}_x)$ all of which must be optimal. Therefore, unlike the case above, we could assign either $(\boldsymbol{\beta}_{x+r_\tau}, \boldsymbol{\gamma}_x) = (\boldsymbol{\beta}, \boldsymbol{\gamma})$ or $(\boldsymbol{\beta}_{x+r_\tau}, \boldsymbol{\gamma}_x) = (\boldsymbol{\gamma}, \boldsymbol{\beta})$ independently (or randomly) for each $r_\tau = 0, 1, 2, \ldots, N-1$.

These various different procedures could be applied similarly when $k > 2$. The following example is for the case where $k = 2$ and $m > 1$.

Example 3: Let $N = 5$. Then, there exists a 4×5 circular Florentine array given as

$$\begin{aligned}
\pi_1 &= (0, 1, 2, 3, 4),\\
\pi_2 &= (0, 2, 4, 1, 3),\\
\pi_3 &= (0, 3, 1, 4, 2),\\
\pi_4 &= (0, 4, 3, 2, 1).
\end{aligned} \tag{16}$$

Any two of the above can be used in the following construction for an optimal pair of perfect sequences of length $mN^2 = 25m$.

Let $m = 3$ and consider the following optimal pair of sequences of length $m = 3$: $\boldsymbol{\beta} = \{1, \omega_3, \omega_3\}$, and $\boldsymbol{\gamma} = \{1, \omega_3^2, \omega_3^2\}$. We choose a 2×5 circular Florentine array $\Pi = \{\pi, \sigma\}$ as $\pi = \pi_1$ and $\sigma = \pi_2$ from (16). Observe that their ranges are the same. Then, for each $r_\tau = 0, 1, 2, 3, 4$, the set $\Psi_{\pi,\sigma}(r_\tau)$ contains $0, 1, 2, 3, 4$, respectively. Therefore, we have $N = 5$ optimal pairs:

$$\begin{aligned}
&(\boldsymbol{\beta}_0, \boldsymbol{\gamma}_0),\\
&(\boldsymbol{\beta}_2, \boldsymbol{\gamma}_1),\\
&(\boldsymbol{\beta}_4, \boldsymbol{\gamma}_2),\\
&(\boldsymbol{\beta}_1, \boldsymbol{\gamma}_3),\\
&(\boldsymbol{\beta}_3, \boldsymbol{\gamma}_4).
\end{aligned}$$

Now, the simple and constant assignment gives $\boldsymbol{\beta}_i = \boldsymbol{\beta}$ and $\boldsymbol{\gamma}_j = \boldsymbol{\gamma}$ for all i and j. An alternative assignment would be, for example,

$$\begin{aligned}
(\boldsymbol{\beta}_0, \boldsymbol{\gamma}_0) &= (\boldsymbol{\beta}, \boldsymbol{\gamma}),\\
(\boldsymbol{\beta}_2, \boldsymbol{\gamma}_1) &= (\boldsymbol{\gamma}, \boldsymbol{\beta}),\\
(\boldsymbol{\beta}_4, \boldsymbol{\gamma}_2) &= (\boldsymbol{\gamma}, \boldsymbol{\beta}),\\
(\boldsymbol{\beta}_1, \boldsymbol{\gamma}_3) &= (\boldsymbol{\beta}, \boldsymbol{\gamma}),\\
(\boldsymbol{\beta}_3, \boldsymbol{\gamma}_4) &= (\boldsymbol{\beta}, \boldsymbol{\gamma}).
\end{aligned}$$

Any of these procedures (assignments) will produce an optimal pair of perfect sequences of length 75.

In Example 3, we have assumed that π and σ have the same range so that Corollary 2 can be applied. Note that they can

TABLE II
SOME EXAMPLES WHERE $\mathcal{O}_{\mathrm{M}}(L) > p_{\min} - 1 = 2$

N	m	$L = mN^2$	$\mathcal{O}_{\mathrm{M}}(L)$	$\mathcal{F}_c(N)$	$p_{\mathrm{m}} - 1$
15	1	225	4	4	-
	5	1125			4
	7	1575			6
	11	2475			10
	13	2925			12
	17	3875			16
	19	4275			18
21	1	441	$\mathcal{F}_c(N)$	$5 \le \mathcal{F}_c(N) \le 19$	-
	5	2250	4		4
	7	3087	$5 \le \mathcal{O}_{\mathrm{M}}(L) \le 6$		6
	11	4851	$5 \le \mathcal{O}_{\mathrm{M}}(L) \le 10$		10
27	1	729	$\mathcal{F}_c(N)$	$4 \le \mathcal{F}_c(N) \le 26$	-
	5	3645	4		4
33	1	1089	$\mathcal{F}_c(N)$	$3 \le \mathcal{F}_c(N) \le 30$	-
	5	5445	$3 \le \mathcal{O}_{\mathrm{M}}(L) \le 4$		4
39	1	1521	$\mathcal{F}_c(N)$	$3 \le \mathcal{F}_c(N) \le 38$	-
	5	7605	$3 \le \mathcal{O}_{\mathrm{M}}(L) \le 4$		4

still be permutations of $\mathbb{Z}_N$ when reduced mod N, even if their ranges over $\mathbb{Z}_{mN}$ are different. In the case where the ranges are different, one must be careful of applying the condition in Theorem 3 (instead of those in Corollary 2).

Theorem 4: Let $\mathcal{F}_c(N)$ denote the largest integer such that an $\mathcal{F}_c(N) \times N$ circular Florentine array exists. Denote by $\mathcal{O}_{\mathrm{GM}}(L)$ the maximum set size of optimal generalized Milewski sequences of period $L = mN^2$ constructed by perfect sequences of period m.

1) If $m = 1$, then

$$\mathcal{O}_{\mathrm{GM}}(mN^2) = \mathcal{F}_c(N).$$

2) If $m \ge 2$, then

$$\mathcal{O}_{\mathrm{GM}}(mN^2) = \min\left\{\mathcal{O}_{\mathrm{P}}(m), \mathcal{F}_c(N)\right\},$$

where $\mathcal{O}_{\mathrm{P}}(m)$ denotes the maximum set size of optimal perfect sequences of period m.

Remark 5: A condition on optimal pairs of Zadoff-Chu sequence was analyzed by Popovic [34]. It is known [34] that the maximum size of optimal Zadoff-Chu sequence sets with period m is $p_{\mathrm{m}} - 1$, where p_{m} is the smallest prime factor of m. As a consequence, there is no optimal pair of Zadoff-Chu sequence if m is even.

By applying Remark 5 to Theorem 4, we get the following corollary on optimal sets of generalized Milewski polyphase sequences of length mN^2 constructed by using Zadoff-Chu sequences of square-free length m. It describes the maximum possible size of optimal sets constructed by using any *known* perfect polyphase sequences.

Corollary 3: Let $\mathcal{O}_{\mathrm{M}}(L)$ be the maximum size of optimal sets of generalized Milewski polyphase sequences of length $L = mN^2$ constructed by using Zadoff-Chu sequences of length m. When $L = mN^2$ is even, $\mathcal{O}_{\mathrm{M}}(L) = 1$, and hence, there is no optimal pair of generalized Milewski polyphase sequences of even length constructed by using Zadoff-Chu sequences. When $L = mN^2$ is odd, we have the following:

1) If $m = 1$, then

$$\mathcal{O}_{\mathrm{M}}(mN^2) = \mathcal{F}_c(N).$$

2) If $m \ge 2$, then

$$\mathcal{O}_{\mathrm{M}}(mN^2) = \min\left\{p_{\mathrm{m}} - 1, \mathcal{F}_c(N)\right\}.$$

where p_{m} is the smallest prime factor of m.

Proof: The proof is obvious for odd mN^2 because of Theorem 4. Assume that the period $L = mN^2$ is even, and observe the following: (1) If m is even, then $p_{\mathrm{m}} - 1 = 1$, and hence, there is no optimal pair of Zadoff-Chu sequences; (2) If N is even, then $\mathcal{F}_c(N) = 1$. [16] ∎

By using the possible values of $\mathcal{F}_c(N)$ given in [37] and $p_{\mathrm{m}} - 1$ from Remark 5, we can find some cases where $\mathcal{O}_{\mathrm{M}}(L = mN^2)$ is larger than $p_{\min} - 1$ by Cor. 3. Table II shows the values of $\mathcal{O}_{\mathrm{M}}(L)$, $\mathcal{F}_c(N)$ and $p_{\mathrm{m}} - 1$, for various values of $L = mN^2$ for $N = 15, 21, 29, 33$ and 39. Recall that p_{m} is the smallest prime factor of m and that p_{mim} is the smallest prime factor of $L = mN^2$.

IV. CONCLUDING REMARKS

Circular Florentine arrays and related combinatorial structures have been studied for more than 30 years to construct sets of non-binary sequences which are optimal in terms of Hamming correlation. They are closely related with edge-decomposition of perfect direct graphs. It is extremely interesting that this structure reappears as an ingredient of constructing optimal sets of perfect sequences in terms of complex correlation. It is all the more interesting to see that, for even N, non-existence of a $2 \times N$ circular Florentine array (proved in [16]) implies non-existence of an optimal pair of generalized Milewski sequences of length mN^2 for any m.

To obtain an optimal k-set of generalized Milewski sequences of period mN^2, it is required to have both a $k \times N$ circular Florentine array and at least one optimal k-sets of perfect sequences of period m. So, to construct large size

$mN_1^2N_2 \times N_2$ array representation

$$\begin{bmatrix} s_0(0) & s_1(0) & \cdots & s_{N_2-1}(0) \\ s_0(1) & s_1(1) & \cdots & s_{N_2-1}(1) \\ \vdots & \vdots & \ddots & \vdots \\ s_0(mN_1^2N_2-1) & s_1(mN_1^2N_2-1) & \cdots & s_{N_2-1}(mN_1^2N_2-1) \end{bmatrix}$$

$\Downarrow$

$mN \times N$ array representation

$$\begin{bmatrix} s_0(0) & s_1(0) & \cdots & s_{N_2-1}(0) & s_0(1) & \cdots & s_{N_2-1}(N_1-1) \\ s_0(N_1) & s_1(N_1) & \cdots & s_{N_2-1}(N_1) & s_0(N_1+1) & \cdots & s_{N_2-1}(2N_1-1) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ s_0((mN-1)N_1) & s_1((mN-1)N_1) & \cdots & s_{N_2-1}((mN-1)N_1) & s_0((mN-1)N_1+1) & \cdots & s_{N_2-1}(mNN_1-1) \end{bmatrix}$$

Fig. 3. Two array representation of a generalized Milewski sequence of length mN^2 constructed by using perfect sequences of length mN_1^2.

optimal sets of generalized Milewski sequences, the following would be interesting:

- For a given integer N, what is the exact value of $\mathcal{F}_c(N)$? This is widely open for non-prime odd integers N except for some small values.
- For a given integer m, what is the exact value of $\mathcal{O}_{\mathrm{P}}(m)$? This value is not known exactly for all $m \geq 2$ but is always greater than or equal to $p_{\mathrm{m}} - 1$, where p_{m} is the smallest prime factor of m. It is equal to $p_{\mathrm{m}} - 1$ when the sequences are restricted to Zadoff-Chu sequences of period m.

APPENDIX A
PROOF OF THEOREM 2

Before we begin the proof, we fix the following notation:

- $N = N_1N_2$ is a composite number.
- π is a function from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$ such that $\pi(x) \pmod N$ is a permutation over $\mathbb{Z}_N$.
- σ is a function from $\mathbb{Z}_{N_2}$ to $\mathbb{Z}_{mN_1^2N_2}$ such that $\sigma(x) \pmod{N_2}$ is a permutation over $\mathbb{Z}_{N_2}$.
- $\kappa_0, \kappa_1, \ldots, \kappa_{N_1-1}$ are functions from $\mathbb{Z}_{N_1}$ to $\mathbb{Z}_{mN_1}$ such that, for each $b = 0, 1, \ldots, N_1 - 1$, $\kappa_b(x) \pmod{N_1}$ is a permutation over $\mathbb{Z}_{N_1}$.

1) To prove the first statement, let $\boldsymbol{s} = \mathcal{I}(\mathcal{S}(G, \sigma, \boldsymbol{\mu})) = \mathcal{I}(\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{N_2-1})$ be a generalized Milewski sequence of period mN^2, constructed by using a collection of N_2 perfect sequences of length mN_1^2, denoted by $G = \{\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{N_2-1}\}$. Here, the i-th column sequence $\boldsymbol{s}_i$ is

$$\boldsymbol{s}_i = \left\{ g_i(t)\mu(i)\omega_{mN_1^2N_2}^{t\sigma(i)} \right\}_{t=0}^{mN_1^2N_2}.$$

The sequence $\boldsymbol{s}$ can be written as two different arrays in Fig. 3: (1) an $mN_1^2N_2 \times N_2$ array in which the r-th column sequence is $\boldsymbol{s}_r$ and; (2) an $mN \times N$ array. For an integer l with $0 \leq l < N$, write $l = aN_2 + b$ with $0 \leq b < N_2$. Then, the l-th column sequence of the second array form is

$$\{s_b(tN_1 + a)\}_{t=0}^{mN-1},$$

where

$$s_b(tN_1 + a) = g_b(tN_1 + a)\mu'(b)\omega^{t\sigma(b)}, \tag{17}$$

and $\mu'(b) = \mu(b)\omega_{mN_1^2N_2}^{a\sigma(b)}$.

Assume that $\boldsymbol{g}_b = \mathcal{I}(\mathcal{S}(B_b, \kappa_b, \boldsymbol{\nu}_b))$ is a generalized Milewski sequence of length mN_1^2 constructed by using $B_b = \{\boldsymbol{\gamma}_{b,0}, \boldsymbol{\gamma}_{b,1}, \ldots, \boldsymbol{\gamma}_{b,N_1-1}\}$, which is a collection of N_1 perfect sequences. Then, the sequence $\boldsymbol{s}$ above becomes a result of the two-step method. By the definition, we can write the term $g_b(tN_1 + a)$ in (17) as

$$g_b(tN_1 + a) = \gamma_{b,a}(t)\nu_b(a)\omega_{mN_1}^{t\kappa_b(a)} \tag{18}$$

After substituting (18) into (17), t-th term of the l-th column sequence in the $mN \times N$ array form in Fig. 3 becomes, for some $\boldsymbol{\mu}'' \in \mathcal{U}_N$,

$$s_b(tN_1 + a) = \gamma_{b,a}(t)\mu''(l)\omega^{t[\sigma(b)+N_2\kappa_b(a)]}. \tag{19}$$

Then, it is easy to see that we can obtain this sequence from the direct method by letting a collection B of N perfect sequences $\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}$ and the function π as follows: (1) $\beta_l(t) = \gamma_{b,a}(t)$ and $\pi(l) = \sigma(b) + N_2\kappa_b(a)$.

2) For the second statement, it is enough to observe that, for any composite number N, there always exists a permutation over $\mathbb{Z}_N$ which cannot be represented by the form

$$\sigma(b) + N_2\kappa_b(a).$$

Note that this form is the exponent of ω in (19).

REFERENCES

[1] *Physical Channels and Modulation (Release 13)*, document TS 36.211 V13.4.0, 3GPP, Jan. 2017.

[2] *Global Positioning Systems Directorate Systems Engineering & Integration Interface Specification*, document IS-GPS-200H, Mar. 2014.

[3] W. Alltop, "Decimations of the Frank-Heimiller sequences," *IEEE Trans. Commun.*, vol. COM-32, no. 7, pp. 851–853, Jul. 1984.

[4] J. J. Benedetto, I. Konstantinidis, and M. Rangaswamy, "Phase-coded waveforms and their design," *IEEE Signal Process. Mag.*, vol. 26, no. 1, pp. 22–31, Jan. 2009.

[5] L. Bomer and M. Antweiler, "Perfect N-phase sequences and arrays [spread spectrum communication]," *IEEE J. Sel. Areas Commun.*, vol. 10, no. 4, pp. 782–789, May 1992.

[6] S. Boztaş and U. Parampalli, "Nonbinary sequences with perfect and nearly perfect autocorrelations," in *Proc. IEEE Int. Symp. Inf Theory*, Austine, TX, USA, Jun. 2010, pp. 1300–1304.

[7] S. Boztaş, F. Özbudak, and E. Tekin, "Generalized nonbinary sequences with perfect autocorrelation, flexible alphabets and new periods," *Cryptogr. Commun.*, vol. 10, no. 3, pp. 509–517, May 2018.

[8] D. Chu, "Polyphase codes with good periodic correlation properties (corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 4, pp. 531–532, Jul. 1972.

[9] W. Chu, S. W. Golomb, and H.-Y. Song, "Tuscan squares," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL, USA: CRC Press, 2007, pp. 652–657.

[10] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 206–209, Jan. 1989.

[11] C. J. Colbourn and J. H. Dinitz, *CRC Handbook of Combinatorial Designs*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2007.
[12] C. Ding, F. Fu, T. Kløve, and V. K.-W. Wei, "Constructions of permutation arrays," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 977–980, Apr. 2002.
[13] P. Fan and M. Darnell, *Sequence Design for Communication Applications*. Hoboken, NJ, USA: Wiley, 1996.
[14] R. L. Frank and S. Zadoff, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory*, vol. 8, no. 6, pp. 381–382, Oct. 1962.
[15] E. M. Gabidulin, "Non-binary sequences with the perfect periodic autocorrelation and with optimal periodic cross-correlation," in *Proc. IEEE Int. Symp. Inf. Theory*, San Antonio, TX, USA, Jan. 1993, p. 412.
[16] S. W. Golomb, T. Etzion, and H. Taylor, "Polygonal path constructions for Tuscan-κ squares," *Ars Combin.*, vol. 30, pp. 97–140, Dec. 1990.
[17] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[18] S. W. Golomb and H. Taylor, "Tuscan squares—A new family of combinatorial designs," *Ars Combinatoria*, vol. 20, pp. 115–132, Dec. 1985.
[19] R. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory*, vol. 7, no. 4, pp. 254–257, Oct. 1961.
[20] T. Høholdt and J. Justesen, "Ternary sequences with perfect periodic autocorrelation (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 4, pp. 597–600, Jul. 1983.
[21] W.-W. Hu, S.-H. Wang, and C.-P. Li, "Gaussian integer sequences with ideal periodic autocorrelation functions," *IEEE Trans. Signal Process.*, vol. 60, no. 11, pp. 6074–6079, Nov. 2012.
[22] V. P. Ipatov, "Multiphase sequences spectrums," *Bull. Higher Educ. Inst. Radioelectron.*, vol. 22, no. 9, pp. 80–82, Jan. 1979.
[23] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combinat. Theory A*, vol. 40, no. 1, pp. 90–107, 1985.
[24] X. Li, P. Fan, and W. H. Mow, "Existence of ternary perfect sequences with a few zero elements," in *Proc. 5th Int. Workshop Signal Design Appl. Commun. (IWSDA)*, Guilin, China, Oct. 2011, pp. 88–91.
[25] C.-D. Lee and S.-H. Hong, "Generation of long perfect Gaussian integer sequences," *IEEE Signal Process. Lett.*, vol. 24, no. 4, pp. 515–519, Apr. 2017.
[26] N. Levanon and E. Mozeson, *Radar Signals*. Hoboken, NJ, USA: Wiley, 2004.
[27] H. D. Luke, "Sequences and arrays with perfect periodic correlation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 24, no. 3, pp. 287–294, May 1988.
[28] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," *IBM J. Res. Develop.*, vol. 27, no. 5, pp. 426–431, Sep. 1983.
[29] W. H. Mow, "A study of correlation of sequences," Ph.D. dissertation, Division Inf. Eng., Chin. Univ. Hong Kong, Hong Kong, 1993.
[30] W. H. Mow, "On the decimations of Frank sequences," *IEEE Trans. Commun.*, vol. 43, nos. 2–4, pp. 751–753, Feb. 1995.
[31] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," in *Proc. IEEE 4th Int. Symp. Spread Spectr. Techn. Appl.*, vol. 3, Mainz, Germany, Sep. 1996, pp. 955–959.
[32] K.-H. Park, H.-Y. Song, D. S. Kim, and S. W. Golomb, "Optimal families of perfect polyphase sequences from the array structure of fermat-quotient sequences," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 1076–1086, Feb. 2016.
[33] S. C. Pei and K. W. Chang, "Perfect Gaussian integer sequences of arbitrary length," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1040–1044, Aug. 2015.
[34] B. M. Popovic, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1406–1409, Jul. 1992.
[35] D. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 6, pp. 720–724, Nov. 1979.
[36] H.-Y. Song, "On aspects of Tuscan squares," Ph.D. dissertation, Dept. EE-Syst., Univ. Southern California, Los Angeles, CA, USA, 1991.
[37] H.-Y. Song, "The existence of circular Florentine arrays," *Comput. Math. Appl.*, vol. 39, no. 11, pp. 31–36, Jun. 2000.
[38] H.-Y. Song and J. H. Dinitz, "Tuscan squares," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL, USA: CRC Press, 1996, pp. 480–484.
[39] H.-Y. Song and S. W. Golomb, "Generalized Welch-Costas sequences and their application to Vatican arrays," in *Finite Fields: Theory, Algorithms Application* (Contemporary Mathematics), vol. 168, G. L. Mullen and P. J.-S. Shiue, Eds. Providence, RI, USA: American Mathematical Society, 1994, pp. 341–351.
[40] H.-Y. Song and J. B. Lee, "On (n, k)-sequences," *Discret Appl. Math.*, vol. 105, nos. 1–3, pp. 183–192, Oct. 2000.
[41] M. K. Song and H.-Y. Song, "A construction of odd length generators for optimal families of perfect sequences," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2901–2909, Apr. 2018.
[42] M. K. Song and H.-Y. Song, "A generalized Milewski construction for perfect sequences," in *Proc. Sequences Their Appl.*, Hong Kong, Oct. 2018, pp. 1–24.
[43] M. K. Song and H.-Y. Song, "Optimal families of perfect polyphase sequences from cubic polynomials," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E101.A, no. 12, pp. 2359–2365, Dec. 2018.
[44] N. Suehiro and M. Hatori, "Modulatable orthogonal sequences and their application to SSMA systems," *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 93–100, Jan. 1988.
[45] X. Tang and G. Gong, "New constructions of binary sequences with optimal autocorrelation value/magnitude," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1278–1286, Mar. 2010.
[46] F. Zeng, X. Zeng, Z. Zhang, and G. Xuan, "Perfect 16-QAM sequences and arrays," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E95.A, no. 10, pp. 1740–1748, 2012.

Min Kyu Song (Member, IEEE) received the B.S. degree in electronic engineering from Konkuk University in 2011, and the M.S. and Ph.D. degrees from Yonsei University in 2013 and 2019, respectively. He is currently working as a Senior Researcher at Agency for Defence Development, South Korea. His research interest includes coding theory (PN sequences and algebraic codes) and their application to digital communication systems.

Hong-Yeop Song (Senior Member, IEEE) received the B.S. degree in electronic engineering from Yonsei University, Seoul, South Korea, in 1984, and the M.S.E.E. and Ph.D. degrees from the University of Southern California, Los Angeles, CA, USA, in 1986 and 1991, respectively. He spent two years as a Research Associate at USC and then two years as a Senior Engineer in standard team of Qualcomm Inc., San Diego, CA. Since September 1995, he has been with the Department of Electrical and Electronic Engineering, Yonsei University. His research interests include digital communications and channel coding, design, and analysis of various pseudo-random sequences for communications and cryptography. He is a member of Mathematical Association of America (MAA) and domestic societies KICS, IEIE, KIISC, and KMS. He was awarded the 2017 Special Contribution Award from Korean Mathematical Society for his contribution to the global wide-spread of the fact that S. J. Choi (1646–1715) from South Korea had discovered a pair of orthogonal Latin squares of order nine much earlier than Euler. He has been serving for IEEE IT Society Seoul Chapter as the Chair from 2009 to 2016. He served as the General Co-Chair for IEEE ITW 2015, Jeju, South Korea.