A Construction of Odd Length Generators for Optimal Families of Perfect Sequences

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

Dedicated to the memory of Solomon W. Golomb (1932-2016)

***Abstract*— In this paper, we give a construction of optimal families of N-ary perfect sequences of period N^2, where N is a positive odd integer. For this, we re-define perfect generators and optimal generators of any length N which were originally defined only for odd prime lengths by Park, Song, Kim, and Golomb in 2016, but investigate the necessary and sufficient condition for these generators for arbitrary length N. Based on this, we propose a construction of odd length optimal generators by using odd prime length optimal generators. For a fixed odd integer N and its odd prime factor p, the proposed construction guarantees at least $(N/p)^{p-1}\phi(N/p)\phi(p)\phi(p-1)/\phi(N)^2$ inequivalent optimal generators of length N in the sense of constant multiples, cyclic shifts, and/or decimations. Here, $\phi(\cdot)$ is Euler's totient function. From an optimal generator one can construct lots of different N-ary optimal families of period N^2, all of which contain $p_{\min}-1$ perfect sequences, where $p_{\min}$ is the least positive prime factor of N.**

***Index Terms*— Perfect polyphase sequences, optimal families of perfect sequences, perfect generators, optimal generators.**

I. Introduction

IN MODERN communication systems and radar systems, sequences with good correlation are widely employed for various purpose such as synchronization [1], multiple access [4], [7], [9], ranging [2], [12]. One of the most well-known example is the direct sequence spread spectrum (DSSS) system, in which each transmitter uses a unique sequence as its signature.

Many of these applications modulate signals by PSK-modulated sequences. Such sequences are called polyphase sequences (or sometimes referred to root-of-unity sequences) since each symbol has unit magnitude and different phase. Those applications use correlations to measure similarity of two sequences. The measurement is called autocorrelation when it is from a sequence and its shifted replica, and is called crosscorrelation when it is from a sequence and the shifted replica of another. Under the noise-free scenario, the autocorrelation with no time shift is always maximum, which is equal to the power allocated to the sequence, and, in other cases, the magnitude is non-negative and can not exceed the allocated power. Thus, to distinguish different sequences and extract desired signal from noise and other signals, it is important to minimize out-of-phase autocorrelation and/or all possible crosscorrelations.

Sequences whose out-of-phase autocorrelations have zero magnitude at any time delay have attracted special interest and they are usually called *perfect sequences.* During about past five decades, many classes of perfect sequences have been reported. There are four well-known and important classes of perfect sequences: 1) the generalized Frank sequence [8], 2) the generalized chirp-like (GCL) sequence [18], which includes the Zadoff-Chu sequence [5], 3) the Milewski sequence [13], and 4) the perfect polyphase sequence associated with the generalized bent function due to Chung and Kumar [6]. And there have been some trials to unify perfect sequence constructions [14], [16].

In parallel, analysis on the crosscorrelation among perfect sequences have also been investigated. There are some theoretical limits on the maximum non-trivial correlation magnitude of a set of sequences [19], [21]. Sarwate bound [19] says that the maximum crosscorrelation between any two perfect sequences of the same length always has magnitude greater than or equal to the square root of the length. Perfect sequence families, which achieve the Sarwate bound, are referred to *optimal perfect sequence families,* or simply, *optimal families.* Lots of constructions for optimal families in the sense of the Sarwate bound have been proposed, e.g., [3], [14], [15], [17], [18], [20]. These results are based on the Frank sequences [3], [15], [20], the GCL sequences [18], and Mow's first unified construction [14], etc.

Recently, in 2016, Park, Song, Kim, and Golomb proposed a construction for optimal sets of p-ary perfect sequences of period p^2, where p is an odd prime [17]. For the family construction, they introduced two important concepts of *perfect generators* and *optimal generators* for generating or constructing perfect sequences and optimal families, respectively. This construction generates a large number of inequivalent optimal families which are more than and covering the previous optimal families based on the Frank sequences such as [3], [15], and [20] at the same parameter. However, there is a restriction: constructed perfect sequences and optimal families are p-ary sequences of periods p^2 ONLY for odd prime p.

In this paper we propose a construction for optimal N-ary perfect sequence families of period N^2, where N is an odd integer. The proposed construction is an extension of the result in [17]. For the purpose, we first generalize the concepts of perfect and optimal generators in Section II. In Section III,

Manuscript received May 31, 2017; revised January 24, 2018; accepted January 24, 2018. Date of publication February 5, 2018; date of current version March 15, 2018. This work was supported by the National Research Foundation of Korea Grant through the Korea Government (MSIP) under Grant 2017R1A2B4011191. This paper was presented in part at the 2017 International Workshop on Signal Design and Its Applications in Communications.

The authors are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, South Korea (e-mail: mk.song@yonsei.ac.kr; hysong@yonsei.ac.kr).

Communicated by T. Helleseth, Guest Editor.

Digital Object Identifier 10.1109/TIT.2018.2801796

we give a connection between the original perfect and optimal generators of odd prime lengths in [17] and some perfect and optimal generators of any odd possible lengths. In this section, as a main result, we propose a construction of optimal generators for optimal N-ary perfect sequence families of period N^2, where N is an odd integer, by using the above connection. Section IV summarizes our results with some concluding remarks.

II. Generators

For convenience, we will use the following notation throughout the paper.

- p is an odd prime and N is a positive integer.
- $\mathbf{x} = \{x(n)\}_{n=0}^{L-1}$ and $\mathbf{y} = \{y(n)\}_{n=0}^{L-1}$ are N-ary sequences of period L. They are (periodic) sequences over the integers mod N. For an integer n, $x(n)$ denotes the n-th term of $\mathbf{x}$.
- $\mathbf{X}$ and $\mathbf{Y}$ are 2-dimensional arrays corresponding to the sequences $\mathbf{x}$ and $\mathbf{y}$, respectively. For example, when $L = ab$, then one period of $\mathbf{x}$ can be written as an $a \times b$ array $\mathbf{X}$ in which the top row is the first b elements of $\mathbf{x}$, second row is the next b elements of $\mathbf{x}$, etc. Sometimes we identify a sequence $\mathbf{x}$ with the array $\mathbf{X}$ corresponding to $\mathbf{x}$.
- $\underline{g}$ is a row vector (or tuple) of certain length over the integers. $\underline{g}^T$ is the column vector obtained by transposing $\underline{g}$. $\underline{g}_i^j$ is a row vector consisting of $j-i+1$ consecutive terms of $\underline{g}$ from i-th to j-th.
- $\mathcal{T}_\tau(\cdot)$ is the τ-shift operator of a sequence $\mathbf{x}$, a vector $\underline{g}$, or an array $\mathbf{X}$, cyclically to the left.
- $\underline{\delta}_N = [0, 1, 2, \ldots, N-1]$. $\underline{1}_N$ and $\underline{0}_N$ are all-one and all-zero vectors of length N, respectively.
- ω_N is a complex primitive N-th root of unity.

A *polyphase sequence* over the circle of radius 1 can be efficiently described by its *phase sequence*. Therefore, in this paper, a 'sequence' means the phase sequence of a certain complex-valued polyphase sequence. We will refer to *the periodic complex correlation* as a 'correlation' and *the periodic Hamming correlation* as a 'Hamming correlation' in this paper, simply.

Let $\mathbf{x}$ and $\mathbf{y}$ be two N-ary sequences of period L. Then, the correlation between $\mathbf{x} = \{x(n)\}_{n=0}^{L-1}$ and $\mathbf{y} = \{y(n)\}_{n=0}^{L-1}$ at time shift τ, denoted by $C_{\mathbf{x},\mathbf{y}}(\tau)$, is given by

$$C_{\mathbf{x},\mathbf{y}}(\tau) = \sum_{n=0}^{L-1} \omega_N^{x(n)-y(n+\tau)},$$

and, the Hamming correlation between $\mathbf{x}$ and $\mathbf{y}$ at time shift τ is

$$H_{\mathbf{x},\mathbf{y}}(\tau) = \sum_{n=0}^{L-1} h\left(x(n), y(n+\tau)\right)$$

where

$$h(a,b) = \begin{cases} 1, & \text{if } a \equiv b \mod N \\ 0, & \text{otherwise.} \end{cases}$$

When $\mathbf{x} = \mathbf{y}$, the above become the autocorrelation, denoted by either $C_{\mathbf{x}}(\tau)$ or $H_{\mathbf{x}}(\tau)$.

Definition 1: Let N be a positive integer.

1) *An N-ary sequence $\mathbf{x}$ of period N^2 is called a 'perfect sequence' if its autocorrelation $C_{\mathbf{x}}(\tau)$ vanishes at all non-trivial shifts $\tau \not\equiv 0 \pmod{N^2}$.*
2) *A pair of N-ary perfect sequences of period N^2 is called an 'optimal pair' if their crosscorrelation magnitude is upper bounded by N at all phase shifts.*
3) *A set of N-ary perfect sequences of period N^2 is called an 'optimal family' if every pair in the set is optimal.*

Consider the interleaved structure of sequences introduced by Gong [10]. For positive integers N and L/N, let $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{N-1}$ be N sequences of length L/N. Then, we obtain a $N \times L/N$ array X by putting $\mathbf{s}_i$ into i-th column of X, i.e.,

$$\mathbf{X} = \left[\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{N-1}\right].$$

By reading the array $\mathbf{X}$ row by row, we obtain an interleaved sequence, denoted by $\mathbf{x}$. For convenience, we write $\mathbf{x}$ as

$$\mathbf{x} = \mathcal{I}\left(\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{N-1}\right) = \mathcal{I}(\mathbf{X}), \tag{1}$$

where $\mathcal{I}$ is the interleaving operator.

Let $\underline{g}$ and $\underline{m}$ be integer vectors of length N. Throughout this paper, we are mainly interested in N-ary perfect sequences of period N^2 of the interleaved form given as

$$\mathbf{x} = \mathcal{I}(\mathbf{X}), \tag{2}$$

where

$$\begin{aligned} \mathbf{X} &= \underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m} \\ &= \Big[g(0)\underline{\delta}_N^T + m(0), g(1)\underline{\delta}_N^T + m(1), \ldots, \\ &\qquad g(N-1)\underline{\delta}_N^T + m(N-1)\Big] \end{aligned} \tag{3}$$

is the corresponding array of $\mathbf{x}$. We would like to note that the sequence $\mathbf{x}$ is fully described by $\underline{g}$ and $\underline{m}$.

An N-tuple $\underline{g}$ in the representation of $\mathbf{x}$ in (2) (or $\mathbf{X}$ in (3)) will be called the generator of $\mathbf{x}$, following the convention in [17]. Park *et al.* [17] studied the generators only of odd prime length p. Main contribution of this paper is to generalize this to a positive integer N which is not necessarily a prime. Following their notation, the *associate family* $\mathcal{S}(\underline{g})$ of $\underline{g}$ is the set of all the N-ary sequences of period N^2 obtained by (2) using all possible $\underline{m}$'s. The terms 'perfect generators' and 'optimal generators' will be used with similar meaning as in [17].

Definition 2 (Perfect Generators): Let N be a positive integer. A generator $\underline{g}$ of length N is a perfect generator if any sequence of period N^2 in the associate family $\mathcal{S}(\underline{g})$ is perfect.

We now prove the necessary and sufficient condition for perfect generators of any positive (even or odd) length $N > 2$. For this, we need the following lemma which describes the relation between $\mathbf{x}$ and its τ-shifted version.

Lemma 1: For a positive integer N, let $\underline{g}$, $\underline{m}$ be vectors of length N and $\mathbf{x}$ be an interleaved sequence in (2)*. Then the τ-shifted version of $\mathbf{x}$ is given as follows.*

Let τ be an integer and $\tau = qN + r$. Then,

$$\mathcal{T}_\tau(\mathbf{x}) = \mathcal{I}\Big(g'(0)\underline{\delta}_N^T + m'(r), g'(0)\underline{\delta}_N^T + m'(0), \ldots, g'(r-1)\underline{\delta}_N^T + m'(r-1)\Big),$$

where $\underline{g}' = \mathcal{T}_r(\underline{g})$ and

$$\underline{m}' = \mathcal{T}_r(\underline{m}) + \Big[\, q\underline{g}_r^{N-1} \;\vdots\; (q+1)\underline{g}_0^{r-1} \,\Big].$$

Proof: It was proven in [10] that $\mathcal{T}_\tau(\mathbf{x})$ is also an interleaved sequence of the form

$$\mathcal{T}_\tau(\mathbf{x}) = \mathcal{I}\left(\mathcal{T}_q(\mathbf{s}_r), \mathcal{T}_q(\mathbf{s}_{r+1}), \ldots, \mathcal{T}_q(\mathbf{s}_{N-1}), \mathcal{T}_{q+1}(\mathbf{s}_0), \mathcal{T}_{q+1}(\mathbf{s}_1), \ldots, \mathcal{T}_{q+1}(\mathbf{s}_{r-1})\right),$$

where $\tau = qN + r$ with $0 \le r < N$. The result follows from this observation easily. ∎

Theorem 1 (Condition on Perfect Generators): Let N be a positive integer. A generator $\underline{g}$ of length N is perfect if and only if $\underline{g}$ is a permutation over the integers modulo N.

Proof: We prove ($\Rightarrow$) only. The other direction has been essentially proved in [11, Th. 3].

Write $n = iN + j$ and $\tau = qN + r$ where $0 \le j, r < N$. By Lemma 1, we write the autocorrelation of $\mathbf{x}$ at delay τ as

$$\begin{aligned}
C_{\mathbf{x}}(\tau) &= \sum_{n=0}^{N^2-1} \omega_N^{x(n)-x(n+\tau)} \\
&= \sum_{j=0}^{N-r-1}\sum_{i=0}^{N-1} \omega_N^{i[g(j)-g(j+r)]+m(j)-m(j+r)-qg(j+r)} \\
&\quad + \sum_{j=N-r}^{N-1}\sum_{i=0}^{N-1} \omega_N^{i[g(j)-g(j+r)]+m(j)-m(j+r)-(q+1)g(j+r)} \\
&= \sum_{j=0}^{N-r-1} \omega_N^{m(j)-m(j+r)-qg(j+r)} \sum_{i=0}^{N-1} \omega_N^{i[g(j)-g(j+r)]} \\
&\quad + \sum_{j=N-r}^{N-1} \omega_N^{m(j)-m(j+r)-(q+1)g(j+r)} \sum_{i=0}^{N-1} \omega_N^{i[g(j)-g(j+r)]}.
\end{aligned}$$

Denote by $\mathcal{A}(r)$ the set of indices $0 \le j \le N-1$ for which $g(j) - g(j+r) = 0$. Then, we have

$$C_{\mathbf{x}}(\tau) = N \sum_{j \in \mathcal{A}(r)} \omega_N^{m(j)-m(j+r)+\theta(j)} \tag{4}$$

for some integer $\theta(j)$ for $j \in \mathcal{A}(r)$.

Assume now that $\underline{g}$ is a perfect generator, and suppose on the contrary that $\underline{g}$ is not a permutation, i.e., some element appears twice or more in $\underline{g}$. Then, it is easily seen that there exists some $r \not\equiv 0 \pmod N$, at which the Hamming autocorrelation of $\underline{g}$ is greater than or equal to 1. This also implies that $|\mathcal{A}(r)| \ge 1$ for some r. In other words, we are now considering the case of some $\tau \not\equiv 0 \pmod{N^2}$ such that $r \not\equiv 0 \pmod N$ and $|\mathcal{A}(r)| \ge 1$.

Now, we consider two sequences $\mathbf{x_1}$ and $\mathbf{x_2}$ generated by the same $\underline{g}$ but with two different $\underline{m}$'s: $\underline{m}_1 = \underline{0}_N$ and $\underline{m}_2$ with only a single non-zero term. Since $\underline{g}$ is perfect, both of these sequences must be perfect, and hence, the correlation of each sequence at all $\tau \not\equiv 0 \pmod{N^2}$ must vanish.

For $\mathbf{x_1}$, we have, for $\tau \not\equiv 0 \pmod{N^2}$, from (4),

$$C_{\mathbf{x_1}}(\tau) = N \sum_{j \in \mathcal{A}(r)} \omega_N^{\theta(j)} = 0. \tag{5}$$

For $\mathbf{x_2}$, we let c be the only non-zero term in position $k \in \mathcal{A}(r)$ of $\underline{m}_2$. Then $k-r$ may or may not belong to $\mathcal{A}(r)$. When $k - r \notin \mathcal{A}(r)$, (4) becomes

$$C_{\mathbf{x_2}}(\tau) = N \sum_{\substack{j \in \mathcal{A}(r),\\ j \ne k}} \omega_N^{\theta(j)} + \omega_N^{c+\theta(k)} = 0.$$

Comparing this with (5), we have

$$\omega_N^{\theta(k)} = \omega_N^{c}\omega_N^{\theta(k)},$$

which is a desired contradiction, since $c \not\equiv 0 \pmod N$. When $k - r \in \mathcal{A}(r)$, we have

$$C_{\mathbf{x_2}}(\tau) = N \sum_{\substack{j \in \mathcal{A}(r),\\ j \ne k,\\ j \ne k-r}} \omega_N^{\theta(j)} + \omega_N^{c+\theta(k)} + \omega_N^{-c+\theta(k-r)} = 0.$$

Comparing this with (5), we have, for any $c \not\equiv 0 \pmod N$,

$$\omega_N^{\theta(k)} + \omega_N^{\theta(k-r)} = \omega_N^{c+\theta(k)} + \omega_N^{-c+\theta(k-r)},$$

which is also a contradiction. ∎

Remark 1: Some comments on Theorem 1 are the following:

1) *The perfect generators of length N in Definition 2 is equivalent to the generalized bent functions over the integers modulo N introduced by Kumar, Scholtz, and Welch in [11, Th. 3].*
2) *The array form of $\mathbf{x}$ given in (3) shows the sum of $\underline{\delta}_N^T\underline{g}$ and $\underline{1}_N^T\underline{m}$. This can be interpreted to be modulating an N-ary sequence $\underline{m}$ of length N with $\underline{g}$. Suehiro and Hatori called such sequences 'modulatable sequences' in [20], and modulatable sequences has been considered in various results on perfect sequence construction [14]–[18]. Because of the connection between perfect sequences and the generalized bent functions, such property has also been considered independently on the construction of generalized bent functions [6], [11]. We would like to note that $\underline{m}$ in Definition 2 can be over the reals without loss of perfectness of the associated sequences of $\underline{g}$. Here, we only consider $\underline{m}$ over the integers.*
3) *Let $\underline{g}$ be an N-ary sequence of length N. Then, $\underline{g}$ is a permutation of $\{0, 1, 2, \ldots, N-1\}$ if and only if the Hamming autocorrelation of $\underline{g}$ is perfect, i.e., for any $\tau \ne 0 \pmod N$,*

$$H_{\underline{g}}(\tau) = \sum_{i=0}^{N-1} h\left(g(i), g(i+\tau)\right) = 0.$$

This gives an alternative condition for $\underline{g}$ to be a perfect generator.

The optimal generators of odd prime length first introduced in [17] is a very special type of the perfect generators. For an odd prime p, let $\underline{g}$ be an optimal generator of length p and u, v be arbitrary chosen two distinct integers in $\{1, 2, \ldots, p-1\}$.

Then, any sequences $\mathbf{x} \in \mathcal{S}(u\underline{g})$ and $\mathbf{y} \in \mathcal{S}(v\underline{g})$, both of length p^2, are not only individually perfect, but also become an optimal pair. An optimal family can thus be constructed by picking up any one sequence from every associate family of the form $\mathcal{S}(u\underline{g})$ for all $u \not\equiv 0 \pmod{p}$. All these ideas will be generalized to arbitrary length N in the remaining of this section.

We first have to investigate the optimality of the pair of sequences from $\mathcal{S}(u\underline{g})$ and $\mathcal{S}(v\underline{g})$, where $\underline{g}$ is a perfect generators of length N. We first have to check if $u\underline{g}$ or $v\underline{g}$ is a perfect generator. It is quite obvious that, when $\underline{g}$ is a permutation of length N, $u\underline{g}$ is also a permutation if and only if u is coprime to N. This is essentially a corollary to Theorem 1.

Corollary 1: Let $\underline{g}$ be a perfect generator of length N. Then, $u\underline{g}$ is perfect of length N if and only if u is coprime to N.

Given a perfect generator $\underline{g}$ of length N, we will consider a pair of sequences $\mathbf{x} \in \mathcal{S}(u\underline{g})$ and $\mathbf{y} \in \mathcal{S}(v\underline{g})$ where u, v are coprime to N. We are in fact interested in very special perfect generators such that such a pair $\mathbf{x}$ and $\mathbf{y}$ becomes an optimal pair of perfect sequences. To make the discussion simple, without loss of generality, we only consider the pair $\mathbf{x} \in \mathcal{S}(\underline{g}')$ and $\mathbf{y} \in \mathcal{S}(u'\underline{g}')$ instead, since letting $u\underline{g} = \underline{g}'$ gives $v\underline{g} = \frac{v}{u}\underline{g}'$. Note that if $\underline{g}$ is a perfect generator, then so is $\underline{g}' = u\underline{g}$ provided that u is coprime to N. Therefore, we now only have to consider the pair of sequences $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$, for any perfect generator $\underline{g}$ and an integer u coprime to N. The following gives a necessary condition for such a pair to be an optimal pair. The necessary condition is that $u-1$ is coprime to N for pairs from $\mathcal{S}(\underline{g})$ and $\mathcal{S}(u\underline{g})$.

Lemma 2: Let $\underline{g}$ be a perfect generator of length N and u be coprime to N. If any pair of sequences $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ is optimal, then $u-1$ is coprime to N.

Proof: Suppose on the contrary that $u-1$ is not coprime to N. We will find a pair of sequences, one from $\mathcal{S}(\underline{g})$ and the other from $\mathcal{S}(u\underline{g})$ whose crosscorrelation is not upper bounded by N. For this we consider $\mathbf{x} \in \mathcal{S}(\underline{g})$ given by

$$\mathbf{x} = \mathcal{I}\left(g(0)\underline{\delta}_N^T, g(1)\underline{\delta}_N^T, \ldots, g(N-1)\underline{\delta}_N^T\right),$$

and its constant multiple $\mathbf{y} = u\mathbf{x} \in \mathcal{S}(u\underline{g})$. The crosscorrelation between $\mathbf{x}$ above and $\mathbf{y} = u\mathbf{x}$ at shift $\tau = 0$ becomes

$$C_{\mathbf{x},u\mathbf{x}}(0) = \sum_{j=0}^{N-1}\sum_{i=0}^{N-1} \omega_N^{(1-u)ig(j)}.$$

Note that the inner sum becomes N if $(1-u)g(j) \equiv 0 \pmod{N}$ and zero otherwise. Now, observe that there are exactly $\gcd(u-1, N)$ values of j such that $(1-u)g(j) \equiv 0 \pmod{N}$ since $\underline{g}$ is a permutation. Therefore,

$$C_{\mathbf{x},\mathbf{y}}(0) = N\gcd(u-1, N).$$

■

An immediate corollary is the non-existence of optimal pairs $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ when $\underline{g}$ is a perfect generator of even length N, since u and $u-1$ cannot both be coprime to an even N.

Corollary 2: Let $\underline{g}$ be a perfect generator of even length N. Then, for any integer u, no pair of sequences $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ is optimal.

We are almost ready to characterize perfect generators $\underline{g}$ such that any pair of sequences $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ becomes an optimal pair, or equivalently, such that any pair of sequences $\mathbf{x} \in \mathcal{S}(u\underline{g})$ and $\mathbf{y} \in \mathcal{S}(v\underline{g})$ becomes an optimal pair. Such a perfect generator will be called an optimal generator in the following definition. We will fix N to be an odd integer in the remaining of this section.

Definition 3 (Optimal Generators): Let N be an odd positive integer.

1) *A perfect generator $\underline{g}$ of length N is an optimal generator if any pair of sequences $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ is an optimal pair for any u such that both u and $u-1$ are coprime to N.*
2) *Given an optimal generator $\underline{g}$, one can construct an optimal family of N-ary perfect sequences of period N^2 by picking up one member from each of the associate families of the form $\mathcal{S}(u_i\underline{g})$, where u_i and $u_i - u_j$ are coprime to N.*

Because of the condition $\gcd(u_i, N) = 1 = \gcd(u_j - u_j, N)$ for all $i \neq j$ in the construction of any optimal family of perfect sequences of period N^2 constructed in Definition 3, the maximum size of such an optimal family cannot exceed the least prime factor of N.

Lemma 3: When we obtain an optimal N-ary perfect sequence family of period N^2 by using an optimal generator in Definition 3, the number of sequences in the family is at most $p_{\min} - 1$, where $p_{\min}$ is the smallest prime factor of N.

Recall that the size of an associate family $\mathcal{S}(u_i\underline{g})$ is at most N^N in general. Thus, there are so many choices even for picking up one member from single associate family. To construct an optimal family, such a choice has to be made at most $p_{\min} - 1$ times. Therefore, a huge number of different optimal families can be constructed for a given N and an optimal generator $\underline{g}$. Furthermore, from Lemma 3, letting $u_i \in \{1, 2, \ldots, p_{\min} - 1\}$ would be enough, but other choices are also possible which would result in different associate families. For example, $u_i = 1$ can be replaced with $u_i' = 1 + p_{\min}$ and this will result in $\mathcal{S}((p_{\min}+1)\underline{g}) \neq \mathcal{S}(\underline{g})$ in general when N is not a prime.

Let $\underline{g}$ be a perfect generator of an odd length N. Let $u \not\equiv 1 \pmod{N}$ be coprime to N so that $u\underline{g}$ is also a perfect generator. Assume that $u-1$ is also coprime to N, and consider a pair of perfect sequences $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ of the form given as

$$\mathbf{x} = \mathcal{I}\Big(g(0)\underline{\delta}_N^T + m_1(0), g(1)\underline{\delta}_N^T + m_1(1), \ldots, g(N-1)\underline{\delta}_N^T + m_1(N-1)\Big) = \mathcal{I}(\mathbf{X}),$$

and

$$\mathbf{y} = \mathcal{I}\Big(ug(0)\underline{\delta}_N^T + m_2(0), ug(1)\underline{\delta}_N^T + m_2(1), \ldots, ug(N-1)\underline{\delta}_N^T + m_2(N-1)\Big) = \mathcal{I}(\mathbf{Y}),$$

where $\underline{m}_1$ and $\underline{m}_2$ are some N-tuples over the integers modulo N. Note that from (3)

$$\mathbf{X} = \underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}_1 \quad \text{and} \quad \mathbf{Y} = \underline{\delta}_N^T u\underline{g} + \underline{1}_N^T \underline{m}_2.$$

Recall that the above pair is optimal if and only if the crosscorrelation is upper bounded by N. To represent the crosscorrelation of $\mathbf{x}$ and $\mathbf{y}$, we write $n = iN + j$ and $\tau = qN + r$ where $0 \le j, r < N$, and follow some similar steps as in the proof of Theorem 1. From Lemma 1,

$$\mathbf{x} - \mathcal{T}_\tau(\mathbf{y}) \equiv \mathcal{I}\left(\underline{\delta}_N^T \left(\underline{g} - u\mathcal{T}_r(\underline{g})\right) - \underline{1}_N^T \underline{m}'\right) \pmod N,$$

where

$$\underline{m}' = \underline{m}_1 - \mathcal{T}_r(\underline{m}_2) - u\left[\, q\underline{g}_r^{N-1} \;\vdots\; (q+1)\underline{g}_0^{r-1} \,\right].$$

Then, the crosscorrelation at τ can be represented as follows:

$$\begin{aligned} C_{\mathbf{x},\mathbf{y}}(\tau) &= \sum_{n=0}^{N^2-1} \omega_N^{x(n)-y(n+\tau)} \\ &= \sum_{j=0}^{N-r-1} \omega_N^{m_1(j)-m_2(j+r)-uqg(j+r)} \sum_{i=0}^{N-1} \omega_N^{i[g(j)-ug(j+r)]} \\ &\quad + \sum_{j=N-r}^{N-1} \omega_N^{m_1(j)-m_2(j+r)-u(q+1)g(j+r)} \\ &\quad \times \sum_{i=0}^{N-1} \omega_N^{i[g(j)-ug(j+r)]} \\ &= N \sum_{j\in\mathcal{B}(r)} \omega_N^{m'(j)}, \end{aligned} \tag{6}$$

where $\mathcal{B}(r)$ is the set of indices $0 \le j \le N-1$ such that $g(j) - ug(j+r) \equiv 0 \pmod N$. We observe that the magnitude of the crosscorrelation given in (6) is upper bounded by N for any $\underline{m}'$ if $|\mathcal{B}(r)| \le 1$ for all r.

Now, we will describe a necessary and sufficient condition for an odd length perfect generator to be an optimal generator as in Definition 3, or, equivalently, the above pair is optimal. It is interesting that the condition is given by the optimality of Hamming crosscorrelation of two perfect generators $\underline{g}$ and $u\underline{g}$ of length N. For the proof, we use the following lemma:

Lemma 4: Let $\underline{g}$ and $\underline{h}$ be N-ary perfect generators of length N. Then,

$$\sum_{r=0}^{N-1} H_{\underline{g},\underline{h}}(r) = N. \tag{7}$$

Proof: LHS is the sum of the number of occurrences of each $g(i)$ in $\underline{h}$ for all i. Since both $\underline{g}$ and $\underline{h}$ are N-ary sequences where every integer mod N appears exactly once, this sum must be N. ∎

Theorem 2 (Condition on Optimal Generators): Let $\underline{g}$ be a perfect generator of an odd length N. Then, $\underline{g}$ is an optimal generator if and only if

$$H_{\underline{g},u\underline{g}}(r) = 1,$$

for any r and any u such that both u and $u-1$ are co-prime to N.

Proof: For sufficiency, we assume that $H_{\underline{g},u\underline{g}}(r) = 1$ for any r from 0 to $N-1$. This implies that $|\mathcal{B}(r)| = 1$ for all r where $\mathcal{B}(r)$ is defined in (6). Therefore, the crosscorrelation of any pair of sequences $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ as described in (6) is upper bounded by N, and hence the pair is optimal. Therefore, $\underline{g}$ is an optimal generator of length N.

For the other direction, assume that $\underline{g}$ is an optimal generator of length N odd. Then both $\underline{g}$ and $u\underline{g}$ are perfect generators and we have, from Lemma 4,

$$\sum_{r=0}^{N-1} H_{\underline{g},u\underline{g}}(r) = N. \tag{8}$$

Now, suppose on the contrary that

$$H_{\underline{g},u\underline{g}}(r_0) \ne 1,$$

for some r_0. From (8), this implies that there exists an integer r_1 such that

$$H_{\underline{g},u\underline{g}}(r_1) \ge 2.$$

This implies in turn that $|\mathcal{B}(r_1)| \ge 2$ when we consider the crosscorrelation of $\mathbf{x} \in \mathcal{S}(\underline{g})$ and $\mathbf{y} \in \mathcal{S}(u\underline{g})$ as described in (6). That is, the crosscorrelation of any such pair is given as (6) with $|\mathcal{B}(r_1)| \ge 2$. This is a desired contradiction since it implies that the pair is not optimal. ∎

Remark 2:

1) *The conditions on perfect generators and optimal generators in [17] for the case of an odd prime N are special cases of Theorem 1 and Theorem 2, respectively.*
2) *The condition in Theorem 2 implies that the Hamming crosscorrelation of $\underline{g}$ and $u\underline{g}$ is 'optimal' for any u with u and $u-1$ coprime to N. It is interesting to observe that the values are all 1 since the sequences $\underline{g}$ and $u\underline{g}$ are permutations of $\{0, 1, 2, \ldots, N-1\}$.*
3) *Figure 1 shows all the relations of generators, perfect generators, and optimal generators in terms of their definitions and in relation to associate families.*

Definition 4: Let $\underline{g}$ be a generator of length N. We define three transformations of N-tuple vectors as follows:

1) *(Constant multiples) Multiplying all the elements of $\underline{g}$ by an integer u co-prime to N.*
2) *(Cyclic shifts) Shifting $\underline{g}$ cyclically to the left by τ.*
3) *(Decimations/Sampling) Decimating $\underline{g}$ by d for d co-prime to N.*

With an abuse of notation, we use any of these transformations for the N-ary sequences of period N^2 similarly.

It is obvious that, for a perfect (or optimal) generator $\underline{g}$ of length N, the result of any of the above transformations of $\underline{g}$ is also a perfect (or optimal) generator of the same length. So, here after, we say that two generators $\underline{g}$ and $\underline{f}$ are equivalent if one can be obtained from the other by applying any combination of the transformations in Definition 4.

Lemma 5: For a positive integer N, let $\underline{g}$, $\underline{m}$ be vectors of length N and $\mathbf{x}$ be an interleaved sequence in (2)*. Then the d-decimated version of $\mathbf{x}$ is given as follows.*

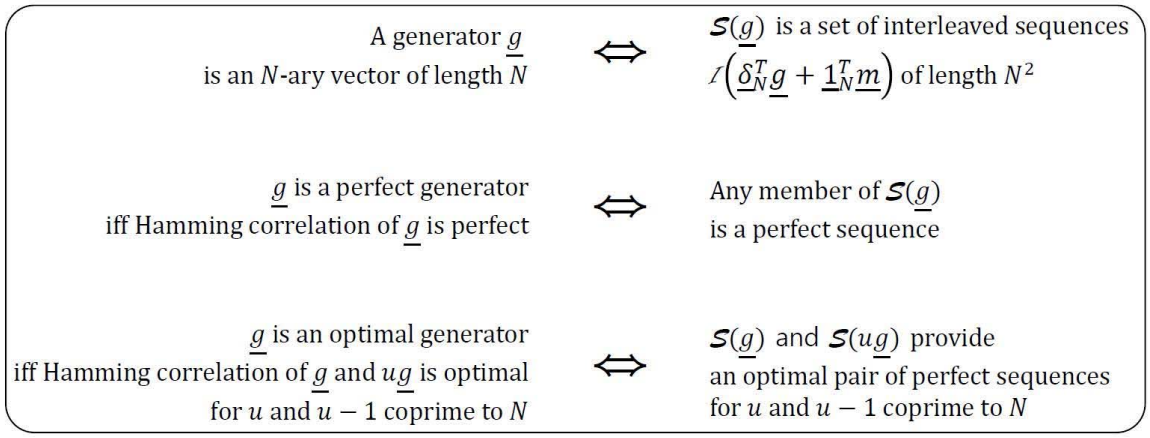

Fig. 1. Relation of generators, perfect generators, and optimal generators in relation to their associate families.

Let d be an integer co-prime to N. Then,

$$\mathcal{D}_d(\mathbf{x}) = \mathcal{I}\left(dg'(0)\underline{\delta}_N^T + m'(0), dg'(1)\underline{\delta}_N^T + m'(1), \ldots, dg'(N-1)\underline{\delta}_N^T + m'(N-1)\right),$$

where $\underline{g}' = \mathcal{D}_d(\underline{g})$ and

$$\underline{m}' = \mathcal{D}_d(\underline{m}) + \left[\lfloor d\frac{0}{N}\rfloor g(0), \lfloor d\frac{1}{N}\rfloor g(d), \ldots, \lfloor d\frac{N-1}{N}\rfloor g(d(N-1))\right].$$

Proof: We consider only the case where $\underline{m} = \underline{0}_N$. If an integer n is written as $n = qN + r$ with $0 \le r < N$, then the n-th term of $\mathbf{x}$ is given as $qg(r)$ from (2). We write $dn = dqN + dr$ and divide dr by N also. This gives

$$dn = \left(dq + \lfloor\frac{dr}{N}\rfloor\right)N + dr - \lfloor\frac{dr}{N}\rfloor N.$$

Since the n-th term of $\mathcal{D}_d(\mathbf{x})$ is the dn-th term of $\mathbf{x}$, and hence, it is given as

$$\left(dq + \lfloor\frac{dr}{N}\rfloor\right)g(dr - \lfloor\frac{dr}{N}\rfloor N) = \left(dq + \lfloor\frac{dr}{N}\rfloor\right)g(dr) = dqg(dr) + \lfloor\frac{dr}{N}\rfloor g(dr),$$

since $\underline{g}$ has period N. ∎

The equivalence relation between perfect sequences from generators can be obtained as a corollary to Lemmas 1 and 5:

Corollary 3: Let $\underline{g}$ and $\underline{f}$ be two perfect generators of the same length. Any two perfect sequences from $\mathcal{S}(\underline{g})$ and $\mathcal{S}(\underline{f})$, respectively, are equivalent if $\underline{g}$ and $\underline{f}$ are equivalent.

III. A Construction for Optimal Generators of Odd Lengths

Our construction for optimal generators of odd lengths is based on the optimal generators of prime lengths. For this, we need to introduce an array representation of an N-tuple vector as 2-dimensional array of size $M \times K$ where $N = MK$ is a factorization of an integer N into two positive factors K and M. We will identify an N-tuple $\underline{g}$ with its $M \times K$ array $\mathbf{G}$ as we have previously identified a sequence $\mathbf{x}$ of period N^2 with its $N \times N$ array $\mathbf{X}$. The following theorem gives a construction for an N-tuple $\underline{g}$ from a K-tuple $\underline{h}$, and $\underline{g}$ is best described by an array of size $M \times K$.

Theorem 3: Let $N = MK$ be a positive integer, λ be a positive integer co-prime to M, and $\underline{\alpha}$ be any K-tuple over the integers. If $\underline{h}$ is a perfect generator of length K, then the N-tuple $\underline{g}$ of length N given by

$$\underline{g} = \mathcal{I}(\mathbf{G}) = \mathcal{I}\left(\lambda K\underline{\delta}_M^T\underline{1}_K + \underline{1}_M^T(\underline{h} + K\underline{\alpha})\right) \tag{9}$$

is a perfect generator.

Proof: It is enough to show that $\underline{g}$ contains all the elements in $\{0, 1, \ldots, N-1\}$ exactly once. For this, we observe that the array form of (9) looks like the following:

$$\mathbf{G} = \lambda K\underline{\delta}_M^T\underline{1}_K + \underline{1}_M^T(\underline{h} + K\underline{\alpha}) = \lambda K\begin{bmatrix}0\\1\\\vdots\\M-1\end{bmatrix}\underbrace{[1,1,\ldots,1]}_{K\text{ times}} + \begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}(\underline{h} + K\underline{\alpha}). \tag{10}$$

Consider the case where $\lambda = 1$ and $\underline{\alpha} = \underline{0}_K$ in (10). Then, it is easily seen that $\underline{g}$ is a permutation of integers mod N since $\underline{h}$ is a permutation of integers mod K. When $\underline{\alpha}$ has a single non-zero term at j-th position, then the corresponding array $\mathbf{G}$ is obtained by appropriately rotating vertically the j-th column of the array with $\underline{\alpha} = \underline{0}_K$. It is obvious therefore that $\underline{g}$ is also such a permutation for any possible values of λ and $\underline{\alpha}$. ∎

Remark 3:

1) *The relation* (9) *gives essentially a construction for $\phi(M)M^K$ permutations of length N from a permutation of length K.*
2) *When we choose $\underline{\alpha} = \underline{0}_K$, $\lambda = 1$, and $\underline{h} = \underline{\delta}_K$, then the generator $\underline{g}$ given by* (9) *is always $\underline{\delta}_N$ whose associate family consists of the Frank sequence of period N^2 [8] and all its modulated versions [20]. Therefore, our construction for optimal generators of odd lengths in Theorem 3 covers the (modulated) Frank sequences.*

Theorem 4: Let $N = MK$ be an odd positive integer. If $\underline{h}$ is an optimal generator of length K, then the generator $\underline{g}$ of length N obtained by (9) *is also an optimal generator.*

Proof: Let $u \not\equiv 1 \pmod N$ and $u-1$ both be coprime to N. The statement can be proved by showing that $H_{\underline{g},u\underline{g}}(r) = 1$ for any r by Theorem 2, or equivalently, that

$$\underline{g} - u\mathcal{T}_r(\underline{g}) \pmod N \tag{11}$$

has only a single 0 for any r.

The case where $r \equiv 0 \pmod N$ is obvious, since

$$\underline{g} - u\mathcal{T}_r(\underline{g}) \equiv (1-u)\underline{g} \pmod N.$$

Similarly to the proof of Lemma 1, it is easy to see that, $\mathcal{T}_r\left(\underline{g}\right)$ is given by

$$\mathcal{T}_r\left(\underline{g}\right) = \mathcal{I}\left(\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(\underline{h}' + K\underline{\alpha}')\right),$$

where $\underline{h}' = \mathcal{T}_s\left(\underline{h}\right)$ and

$$\underline{\alpha}' = \mathcal{T}_s\left(\underline{\alpha}\right) + \left[\, q\underline{1}_{K-s} \vdots (q+1)\underline{1}_s \,\right],$$

and $r = qK + s$ with $0 \le s < K$. Then, (11) becomes

$$\begin{aligned}
&\underline{g} - u\mathcal{T}_r(\underline{g}) \\
&\quad = \mathcal{I}\left(\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(\underline{h} + K\underline{\alpha})\right) \\
&\qquad - \mathcal{I}\left(u\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(u\underline{h}' + uK\underline{\alpha}')\right) \\
&\quad = \mathcal{I}\left((1-u)\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(\underline{h} - u\mathcal{T}_s(\underline{h})) + K\underline{1}_M^T\underline{\alpha}''\right)
\end{aligned} \tag{12}$$

for some K-tuple $\underline{\alpha}''$. We observe that, since $\underline{h}$ is an optimal generator of length K, the K-tuple $\underline{h} - u\mathcal{T}_s(\underline{h}) \pmod K$ has only a single 0. This in turn implies that $\underline{g} - u\mathcal{T}_r(\underline{g})$ has only a single 0 as an N-ary interleaved sequence of length N given by (12). Therefore, $\underline{g}$ is an optimal generator of length N. ■

By Theorem 4, we can construct optimal generators of odd lengths from optimal generators of odd prime lengths already known in [17]:

Fact 1 ([17, Th. 9]): Let p be an odd prime. Let τ be any integer, m be an integer with $m \not\equiv 0 \pmod p$ and k be an integer co-prime to $p-1$. Then, a generator $\underline{h}$ in which the n-th term is given by

$$h(n) = m(n+\tau)^k \tag{13}$$

is an optimal generator of length p. And the number of inequivalent optimal generators of length p obtained from the above is $\phi(p-1)$, where $\phi(\cdot)$ is Euler's totient function.

We are now interested in how many inequivalent optimal generators of length $N = Mp$ from a given optimal generators of length p in Fact 1. Following corollary gives an idea of d-decimation of the generator obtained by (9) in Theorems 3 and 4.

Corollary 4: Let $N = MK$ be a positive odd integer, $\underline{h}$ be a generator of length K, and d be an integer co-prime to N. Then, the array of d-decimation of the generator $\underline{g}$ obtained by (9) is of the form

$$\mathcal{D}_d(\underline{g}) = \mathcal{I}\left(d\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(\underline{h}' + K\underline{\alpha}')\right)$$

where $\underline{h}' = \mathcal{D}_d\left(\underline{h}\right)$ and

$$\underline{\alpha}' = \mathcal{D}_d\left(\underline{\alpha}\right) + \lambda\left[\lfloor d\frac{0}{K}\rfloor, \lfloor d\frac{1}{K}\rfloor, \ldots, \lfloor d\frac{K-1}{K}\rfloor\right].$$

We will clearly state when two generators $\underline{g}_1$ and $\underline{g}_2$ obtained by (9) become equivalent or not in the following corollary to Theorems 3 and 4, and Corollary 4. Recall Definition 4 and equivalence of two generators of the same length.

Corollary 5: Let $\underline{h}_1$ be a perfect generator of length K, and $\underline{g}_1$ be the generator of length $N = MK$ obtained by (9) from $\underline{h}_1$. If $\underline{h}_2$ is not equivalent to $\underline{h}_1$, then any generator $\underline{g}_2$ obtained by (9) from $\underline{h}_2$ are not equivalent to $\underline{g}_1$. Conversely, if $\underline{g}_2$ is equivalent to $\underline{g}_1$, then there exists $\underline{h}_2$ that is equivalent to $\underline{h}_1$ and $\underline{g}_2$ can be obtained by (9) from $\underline{h}_2$.

Theorem 5: Let $N = pM$ be an odd positive integer where p be an odd prime. Denote by $I(N,p)$ the number of inequivalent optimal generators of length N obtained by Theorem 4 using an optimal generator of length p. Then,

$$I(N,p) \ge \frac{\phi(N/p)\phi(p)}{\phi(N)^2}\left(\frac{N}{p}\right)^{p-1}.$$

Since there are $\phi(p-1)$ inequivalent optimal generators of length p from Fact 1, we have at least

$$\frac{\phi(N/p)\phi(p)\phi(p-1)}{\phi(N)^2}\left(\frac{N}{p}\right)^{p-1}$$

inequivalent optimal generators of length N obtained by Theorem 4 and Fact 1.

Proof: The construction in Theorem 4 gives $\phi(M)$ choices for λ and M^p choices for $\underline{\alpha}$ using a single generator of length p. This gives a total of $\phi(M)M^p$ generators of length N from a single generator of length p.

Given any optimal generator of length p, there are $\phi(p)$ constant-multiples and p cyclic-shifts which are all inequivalent to each other. This counts a total of $\phi(p)p$ generators of length p from a given one. Since a decimation may be obtained by some combination of constant-multiple and cyclic-shift, we do not count this here, and hence, a total of at least $p(M)^p\phi(p)\phi(M)$ optimal generators of length N by Theorem 4 from a single optimal generator and all its equivalent ones.

On the other hand, there are N cyclic-shifts, $\phi(N)$ constant-multiples, and $\phi(N)$ decimations of a single generator of length N. This gives the lower bound on $I(N,p)$ in the first expression.

If we use optimal generators of length p from Fact 1, using Corollary 5, we have the second expression by multiplying $\phi(p-1)$ to the above. ■

Example 1: For $N = 9$ and $p = 3$, the lower bound in Theorem 5 is $3^2\phi(3)^2/\phi(9)^2 = 1$. It turned out that there are four inequivalent optimal generators which we can get by the proposed construction in Theorem 4 with an optimal generator of length 3. Table I gives the exhaustive list of all the inequivalent optimal generators of length 9 by this construction.

1) *Note that, when $p = 3$, Fact 1 gives only one optimal generator:* $[0,1,2]$. *Note also that, if we let*

$$\underline{g} = [0,1,2,3,4,5,6,7,8],$$

then $\mathcal{S}(\underline{g})$ consists of the 9-ary Frank sequence of period 9^2 and all its modulated version. Therefore, any optimal

TABLE I

LIST OF ALL THE INEQUIVALENT OPTIMAL GENERATORS OF LENGTH $N = 9$ FROM AN OPTIMAL GENERATOR OF LENGTH $p = 3$

$\underline{h}$	$\underline{g}$
$[0, 1, 2]$	$[0, 1, 2, 3, 4, 5, 6, 7, 8]$
	$[0, 1, 5, 3, 4, 8, 6, 7, 2]$
	$[0, 2, 1, 3, 5, 4, 6, 8, 7]$
	$[0, 2, 4, 3, 5, 7, 6, 8, 1]$

family obtained from this $\underline{g}$ by using the construction in Definition 3 is essentially the same as the optimal perfect sequence family constructed in [20] and [16].

2) *Since we have three additional inequivalent optimal generators of length 9 as shown in Table I, we can construct three additional optimal families of perfect sequences of period $9^2 = 81$ which are new (not mentioned in [20] or [16]). Note that all these optimal families have the same size.*

Example 2: For $N = 15 = 3 \times 5$, there are two choices for an odd prime p.

1) *Choose $p = 5$. Table II shows the exhaustive list of all the inequivalent optimal generators of length 15 constructed by Theorem 3 using all the optimal generators of length 5 from Fact 1. The number of inequivalent optimal generators from an optimal generator of length 5 turned out to be fourteen, while the lower bound is 10.125. The total number of inequivalent optimal generators is twenty-eight, since there are two inequivalent optimal generators of length 5.*
Similar to the case of $p = 3$ and $N = 9$,

$$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]$$

is the generator of the Frank sequence of period $15^2 = 225$ and, by using it, we can get optimal perfect sequence families which is same to the results in [20] and [16]. Since we have twenty-seven more inequivalent optimal generators, we can generate twenty-seven times more optimal sets of perfect sequences of period 225, each of which is of size same to those in [20] and [16].

2) *Choose $p = 3$. Table III shows the exhaustive list of all the inequivalent optimal generators of length 15 from the optimal generator of length 3.*
In this case, all the optimal generators except for

$$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]$$

are inequivalent to those in Table II.
We have constructed a total of $28 + 5 - 1 = 32$ inequivalent optimal generators of length 15 of which 31 of them are new.

TABLE II

LIST OF ALL THE INEQUIVALENT OPTIMAL GENERATORS OF LENGTH $N = 15$ FROM OPTIMAL GENERATORS OF LENGTH $p = 5$

$\underline{h}$	$\underline{g}$
$[0, 1, 2, 3, 4]$	$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]$
	$[0, 1, 2, 3, 9, 5, 6, 7, 8, 14, 10, 11, 12, 13, 4]$
	$[0, 1, 2, 8, 9, 5, 6, 7, 13, 14, 10, 11, 12, 3, 4]$
	$[0, 1, 2, 8, 14, 5, 6, 7, 13, 4, 10, 11, 12, 3, 9]$
	$[0, 1, 7, 8, 4, 5, 6, 12, 13, 9, 10, 11, 2, 3, 14]$
	$[0, 1, 7, 8, 9, 5, 6, 12, 13, 14, 10, 11, 2, 3, 4]$
	$[0, 1, 7, 8, 14, 5, 6, 12, 13, 4, 10, 11, 2, 3, 9]$
	$[0, 1, 7, 13, 4, 5, 6, 12, 3, 9, 10, 11, 2, 8, 14]$
	$[0, 1, 7, 13, 9, 5, 6, 12, 3, 14, 10, 11, 2, 8, 4]$
	$[0, 1, 7, 13, 14, 5, 6, 12, 3, 4, 10, 11, 2, 8, 9]$
	$[0, 6, 7, 8, 9, 5, 11, 12, 13, 14, 10, 1, 2, 3, 4]$
	$[0, 6, 7, 8, 14, 5, 11, 12, 13, 4, 10, 1, 2, 3, 9]$
	$[0, 6, 7, 13, 14, 5, 11, 12, 3, 4, 10, 1, 2, 8, 9]$
	$[0, 6, 12, 13, 9, 5, 11, 2, 3, 14, 10, 1, 7, 8, 4]$
$[0, 1, 3, 2, 4]$	$[0, 1, 3, 2, 4, 5, 6, 8, 7, 9, 10, 11, 13, 12, 14]$
	$[0, 1, 3, 2, 9, 5, 6, 8, 7, 14, 10, 11, 13, 12, 4]$
	$[0, 1, 3, 2, 14, 5, 6, 8, 7, 4, 10, 11, 13, 12, 9]$
	$[0, 1, 3, 7, 4, 5, 6, 8, 12, 9, 10, 11, 13, 2, 14]$
	$[0, 1, 3, 7, 9, 5, 6, 8, 12, 14, 10, 11, 13, 2, 4]$
	$[0, 1, 3, 7, 14, 5, 6, 8, 12, 4, 10, 11, 13, 2, 9]$
	$[0, 1, 3, 12, 4, 5, 6, 8, 2, 9, 10, 11, 13, 7, 14]$
	$[0, 1, 3, 12, 9, 5, 6, 8, 2, 14, 10, 11, 13, 7, 4]$
	$[0, 1, 3, 12, 14, 5, 6, 8, 2, 4, 10, 11, 13, 7, 9]$
	$[0, 1, 8, 12, 4, 5, 6, 13, 2, 9, 10, 11, 3, 7, 14]$
	$[0, 6, 3, 2, 9, 5, 11, 8, 7, 14, 10, 1, 13, 12, 4]$
	$[0, 6, 3, 2, 14, 5, 11, 8, 7, 4, 10, 1, 13, 12, 9]$
	$[0, 6, 3, 7, 9, 5, 11, 8, 12, 14, 10, 1, 13, 2, 4]$
	$[0, 6, 13, 2, 9, 5, 11, 3, 7, 14, 10, 1, 8, 12, 4]$

TABLE III

LIST OF ALL THE INEQUIVALENT OPTIMAL GENERATORS OF LENGTH $N = 15$ FROM OPTIMAL GENERATORS OF LENGTH $p = 3$

$\underline{h}$	$\underline{g}$
$[0, 1, 2]$	$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]$
	$[0, 1, 5, 3, 4, 8, 6, 7, 11, 9, 10, 14, 12, 13, 2]$
	$[0, 4, 5, 3, 7, 8, 6, 10, 11, 9, 13, 14, 12, 1, 2]$
	$[0, 4, 8, 3, 7, 11, 6, 10, 14, 9, 13, 2, 12, 1, 5]$
	$[0, 4, 14, 3, 7, 2, 6, 10, 5, 9, 13, 8, 12, 1, 11]$

IV. CONCLUDING REMARKS

In this paper, we first re-define the concepts of perfect generators and optimal generators. From the new definition, we discuss the necessary and sufficient condition of them by using the property of generators. For any odd integer N and its factor K, we give a connection between optimal generators of length N and optimal generators of length K.

The following are some interesting open problems.

1) For an odd N, find the maximum number of inequivalent optimal generators of length N. Theorem 5 gives a lower bound depending on an odd prime factor of N.
2) A composite integer can have two or more distinct prime factors. Let N be a positive odd integer and assume that p and q are two distinct odd prime factors of N, i.e.,

$$N = pN_1 = qN_2.$$

Then, what is the relationship between two optimal generators of length N, which come from optimal generators of length p and q, respectively? After answering the question, further classification is also interesting. For example, Example 2 gives a complete description of the case where $N = 15$.

3) For a given length N, how many optimal generators are there? By using the proposed construction, can we obtain all the optimal generators of an odd length N? This problem is closely related to Conjecture 1 in [17] on the optimal generators of odd prime length. We do not have any example of an optimal generator of an odd length N which is constructed otherwise.

REFERENCES

[1] *Physical Channels and Modulation (Release 13)*, document 3GPP TS 36.211 V13.4.0, 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. Inf. Theory*, vol. IT-32, no. 7, pp. 851–853, Jul. 1984.

[4] 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.

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

[6] 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.

[7] P. Z. Fan and M. Darnell, *Sequence Design for Communications Applications*. Hoboken, NJ, USA: Wiley, 1996.

[8] R. Frank, S. Zadoff, and R. Heimiller, "Phase shift pulse codes with good periodic correlation properties (Corresp.)," *IRE Trans. Inf. Theory*, vol. 8, no. 6, pp. 381–382, Oct. 1962.

[9] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar*. New York, NY, USA: Cambridge Univ. Press, 2005.

[10] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 400–411, Mar. 1995.

[11] 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.

[12] N. Levanon and E. Mozeson, *Radar Signals*. Hoboken, NJ, USA: Wiley, 2004.

[13] 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.

[14] W. H. Mow, "A study of correlation of sequences," Ph.D. dissertation, Dept. Inf. Eng., Chinese Univ. Hong Kong, Hong Kong, May 1993.

[15] W. H. Mow, "On the decimations of Frank sequences," *IEEE Trans. Commun.*, vol. 43, no. 234, pp. 751–753, Feb. 1995.

[16] 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. Sep. 1996, pp. 955–959.

[17] 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.

[18] 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.

[19] D. V. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 6, pp. 720–724, Nov. 1979.

[20] N. Suehiro and M. Hatori, "Modulatable orthogonal sequences and their application to SSMA systems," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 1, pp. 93–100, Jan. 1988.

[21] L. Welch, "Lower bounds on the maximum cross correlation of signals (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IY-20, no. 3, pp. 397–399, May 1974.

Min Kyu Song (S'14) received his BS degree in Electronic Engineering from Konkuk University, Seoul, Korea, and MS degree in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in 2011 and 2013, respectively. He is currently a Ph.D candidate working in Communication Signal Design Lab. at Yonsei University. His area of research interest includes PN sequences, cryptography, and coding theory.

Hong-Yeop Song (S'85–M'92–SM'07) received his BS degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D degrees from the University of Southern California, Los Angeles, California, in 1986 and 1991, respectively. He spent 2 years as a research associate at USC and then 2 years as a senior engineer at the standard team of Qualcomm Inc., San Diego, California. Since Sept. 1995, he has been with Dept. of electrical and electronic engineering, Yonsei University, Seoul, Korea. He had been serving IEEE IT society Seoul Chapter as a chair from 2009 to 2016, and served as a general co-chair of IEEE ITW 2015 in Jeju, Korea. He was awarded the 2017 Special Contribution Award from Korean Mathematical Society for his contribution to the global wide-spread of the fact that Choi (1646-1715) from Korea had discovered a pair of orthogonal Latin squares of order 9 much earlier than Euler. His area of research interest includes digital communications and channel coding, design and analysis of various pseudo-random sequences for communications and cryptography. He is a member of IEEE, MAA(Mathematical Association of America) and domestic societies KICS, IEIE, KIISC and KMS.