Optimal Families of Perfect Polyphase Sequences From the Array Structure of Fermat-Quotient Sequences

Ki-Hyeon Park, *Student Member, IEEE*, Hong-Yeop Song, *Senior Member, IEEE*, Dae San Kim, *Member, IEEE*, and Solomon W. Golomb, *Life Fellow, IEEE*

***Abstract*— We show that a p-ary polyphase sequence of period p^2 from the Fermat quotients is perfect. That is, its periodic autocorrelation is zero for all non-trivial phase shifts. We call this Fermat-quotient sequence. We propose a collection of optimal families of perfect polyphase sequences using the Fermat-quotient sequences in the sense of the Sarwate bound. That is, the cross correlation of two members in a family is upper bounded by p. To investigate some relation between Fermat-quotient sequences and Frank–Zadoff sequences and to construct optimal families including these sequences, we introduce generators of p-ary polyphase sequences of period p^2 using their $p \times p$ array structures. We call an optimal generator to be the generator of some p-ary polyphase sequences which are perfect and which gives an optimal family by the proposed construction. Finally, we propose an algebraic construction for optimal generators as another main result. A lot of optimal families of size $p-1$ can be constructed from these optimal generators, some of which are known to be from the Fermat-quotient sequences or from the Frank–Zadoff sequences, but some families are new for $p \geq 11$. The relation between the Fermat-quotient sequences and the Frank–Zadoff sequences is determined as a by-product.**

***Index Terms*— Fermat-quotient sequences, Frank-Zadoff sequences, perfect polyphase sequences, generators of perfect sequences, optimal family of perfect sequences.**

I. Introduction

SEQUENCES with good periodic correlation have been widely studied for their application to various communication systems [11], [12], [15], [17], [20], [22], [24]–[26], [28], [31], [38], [41], [45], [46], [48], [51], [52]. For example, direct-sequence spread-spectrum systems employ a single sequence of long period with the side-lobe correlation magnitudes as small as possible (zero, for perfectness), which includes military communication systems requiring the anti-jamming performance [47]. Recent applications include such commercial mobile communication systems as CDMA, WCDMA, and 3GPP LTE [1], [49] and global navigation satellite systems as GPS [2] and GALILEO [13], in which not only a single sequence with good autocorrelation but also a family of sequences with good cross-correlation play an essential role in their performance. Non-binary sequences with good correlation also find application to pulse-compression RADAR or active SONAR [7], [30], [35]. These sequences are also used for the design of sequences with good aperiodic or partial-periodic correlation, which are known to be more important in practice [3], [6], [16], [21], [52].

Most common examples of non-binary sequences are polyphase sequences which have values on the unit circle of the complex plane. These polyphase sequences having complex values with constant unit amplitude have been widely studied to make sequences with the perfect periodic autocorrelation, and to design phase-coded pulses for pulse-compression [29], [34], [36]. Heimiller [25] proposed in 1961 the p-ary polyphase sequence of period p^2 with the zero periodic autocorrelation at all non-trivial phase-shifts (we will call this 'perfect' in this paper), where p is a prime. It turned out that these sequences are included in the sequences proposed much earlier by Frank and Zadoff in which p needs not be a prime, and now it is called Frank-Zadoff sequences [17]. This had been the only perfect sequence until Chu proposed another type: N-ary (for N odd) or $2N$-ary (for N even) polyphase sequences of period N with the zero periodic autocorrelation at all non-trivial phase shifts, where N is a positive integer [11]. Later, this is generalized to chirp-like sequences by Popović [45], and this generalized version was recently adopted to 3GPP LTE standard, which is now called Zadoff-Chu sequences [1, p. 31]. As an effort of reducing the ratio between the number of phases and the length of sequence, Milewski proposed some perfect polyphase sequences with period m^{2k+1} over m^{k+1} phases [40]. These ideas have been generalized for the direction of using a smaller alphabet size by Liu and Fan [37] as well as by Blake and Tirkel [5]. Zhang and Golomb [52] proposed another variation of Chu sequences which is perfect in periodic autocorrelation and favorable aperiodic autocorrelation. Kumar proposed the perfect polyphase sequences as generalized bent functions [31] and Mow unified the constructions of perfect polyphase

Manuscript received April 24, 2015; revised October 25, 2015; accepted December 14, 2015. Date of publication December 23, 2015; date of current version January 18, 2016. This work was supported by the Ministry of Science, ICT and Future Planning under Grant 10047212. This paper was presented at the 2015 IEEE International Symposium on Information Theory. *(Corresponding author: Hong-Yeop Song.)*

K.-H. Park and H.-Y. Song are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, Korea (e-mail: kh.park@yonsei.ac.kr; hysong@yonsei.ac.kr).

D. S. Kim is with the Department of Mathematics, Sogang University, Seoul 121-742, Korea (e-mail: dskim@sogang.ac.kr).

S. W. Golomb is with the Department of Electrical Engineering-Systems, University of Southern California, Los Angeles, CA 90089 USA (e-mail: sgolomb@usc.edu).

Communicated by K. Yang, Associate Editor for Sequences.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2015.2511780

sequences [41]. Recently, Soltanalian and Stoica [48] treated these problems and considered their existence from Mow's results as well as some results of analysis using relative difference sets [39].

The cross-correlation of original Frank-Zadoff sequence is also studied by Suehiro and Hatori [51]. They showed that the sequence family has also optimal cross-correlation in the sense of the lower bound of Sarwate [46] (we will call this 'optimal family' in this paper). Gabidulin [19] generalized these sequences and constructed p^k-ary perfect polyphase sequences of length p^{2k} as well as optimal families with these parameters. The cross-correlation of Zadoff-Chu sequences is studied by Popović [45] with their generalization. Popovic showed also that the sequence family has optimal cross-correlation. Later, the cross-correlation of generalized Zadoff-Chu sequences was studied by Kang *et al.* [27] and is currently being studied by many others [32].

For a long time, the Fermat quotients have been studied extensively because of its numerous characteristics and properties in number theory [8]–[10], [14], [23], [43], [50]. It is interesting to find that, however, most of the results so far have focused on the randomness of the binary sequences derived from them. For example, Chen *et al.* [8] and Chen [9] showed some randomness properties, and Ostafe and Shparlinski [43] studied dynamical systems using Fermat quotients, and proposed its application to communication and cryptography systems. Fermat quotients and binary sequences derived from them are generalized to Euler quotients [10]. Su [50] designed a practical sequence families from the p-ary Fermat-quotient sequences, showing their Hamming correlation property [33] for frequency-hopping spread spectrum systems [4], [18]. Gomez and Winterhof [23] estimated the multiplicative character sums of the p-ary Fermat-quotient sequences.

The remaining part of this paper is organized as follows. In Section II, we will show that a p-ary sequence of period p^2 derived from the Fermat quotients is perfect, which we call the Fermat-quotient sequence, and propose families of p-ary sequences with optimal cross-correlation from this. It is interesting to find that the same construction works for the Frank-Zadoff sequence, both of which are perfect p-ary polyphase sequences of period p^2. As far as all authors are aware of, this is a new observation that the p-ary Fermat-quotient sequence is perfect. All the families in our constructions are, so called, 'completely optimal' in the sense that the cross-correlation of any two members in a family is exactly p for all phase shifts. Our construction is more general since it encloses previously known optimal families from Frank-Zadoff sequences [51] and generates much more different families with the same parameters. We remark that most of this section was presented in [44].

In Section III, we will derive the conditions for an optimal family and present a general approach (Theorem 4) to find optimal families including those from Fermat-quotient or Frank-Zadoff sequences. To do this, we introduce a sequence called a 'generator'. After defining the associated family of certain generators, we derive the condition on the generators (Theorem 5) so that all the sequences in the associated family of the generator are perfect. Moreover, we investigate some properties of the generators (Theorems 6, 7, 8) so that one can form completely optimal families of size $p-1$ by selecting members from certain associated families of the generators. We call such a generator an optimal generator. We give an algebraic construction (Theorem 9) of optimal generators, which gives not only those for Fermat-quotient and Frank-Zadoff sequences but also, for $p \geq 11$, those for some new optimal families by Theorem 4.

In Section IV, we confirm that the construction in this paper covers the families from optimal generators exhaustively by computers for $p \leq 13$. We conclude this paper with some unsolved conjectures, including some relation with Mow's conjecture [41], [48] about the number of perfect polyphase sequences.

II. The p-Ary Fermat-Quotient Sequence of Period p^2 and Its Properties

We begin by defining the correlation of sequences that we will use in this paper. Throughout the paper, we let p be an odd prime and denote by ω a complex primitive p-th root of unity.

Definition 1: Let $\mathbf{u} = \{u(t)|t \in \mathbb{Z}, u(t) \in \mathbb{Z}_p\}$ *and* $\mathbf{v} = \{v(t)|t \in \mathbb{Z}, v(t) \in \mathbb{Z}_p\}$ *be p-ary sequences of period* $N = p^2$. *Then the periodic cross-correlation of* $\mathbf{u}$ *and* $\mathbf{v}$, *when they are cyclically distinct, is defined as*

$$C(\mathbf{u}, \mathbf{v}, \tau) = \sum_{t=0}^{N-1} \omega^{u(t+\tau)-v(t)}, \quad \tau = 0, 1, 2, \ldots. \tag{1}$$

It is called the periodic autocorrelation when $\mathbf{u} = \mathbf{v}$ *or they are cyclically equivalent, and is denoted by* $C(\mathbf{u}, \tau)$. *A sequence* $\mathbf{u}$ *is said to be 'perfect' if its non-trivial periodic autocorrelation is zero. That is,* $C(\mathbf{u}, \tau) = 0$ *for all* $\tau \not\equiv 0 \pmod N$.

A pair of cyclically distinct sequences is said to be 'optimal' if the magnitude of their periodic cross-correlation is upper bounded by $\sqrt{N} = p$ [44], [46] *and if both are perfect. We call such a pair an optimal pair. It is called a 'completely optimal' pair if the magnitude of their periodic cross-correlation is equal to* $\sqrt{N} = p$ *for all phase-shifts and if both are perfect.*

A sequence family $\mathcal{F}$ *is said to be 'optimal' if every pair of distinct members of* $\mathcal{F}$ *is optimal. It is called 'completely optimal' if every pair of distinct members of* $\mathcal{F}$ *is a completely optimal pair.*

Remark 1: Some authors defined a perfect sequence to be the complex root-of-unity sequence $\{\omega^{u(t)}|t \in \mathbb{Z}\}$ *such that the autocorrelation* $C(\mathbf{u}, \tau)$ *in* (1) *is zero for all non-trivial phase shifts. See* [41], [42] *for example. In this paper, instead, we call its p-ary 'phase' sequence* $\mathbf{u} = \{u(t)|t \in \mathbb{Z}, u(t) \in \mathbb{Z}_p\}$ *a perfect sequence.*

Definition 2 [8], [9], [14], [23]: Let

$$Q(t) = \frac{t^{p-1} - 1}{p}$$

where t is an integer with $t \not\equiv 0 \pmod p$. *Define a p-ary Fermat-quotient sequence* $\mathbf{q} = \{q(t)|t \in \mathbb{Z}\}$ *as*

$$q(t) \equiv \begin{cases} Q(t) \pmod p & \text{if } t \not\equiv 0 \pmod p, \\ 0 \pmod p & \text{otherwise.} \end{cases} \tag{2}$$

The following properties of Fermat-quotient sequences are well-known [8], [9], [14], [23].

Lemma 1:

1) $q(t) \equiv q(p^2 \pm t) \pmod p$ *for any integer* t. *Therefore* $\mathbf{q}$ *has period* p^2 *and is palindromic.*
2) $q(tu^{\pm 1}) \equiv q(t) \pm q(u) \pmod p$ *for any integers* t, $u \not\equiv 0 \pmod p$.
3) $q(t + kp) \equiv q(t) - \frac{k}{t} \pmod p$ *for any integer* $t \not\equiv 0 \pmod p$ *and any integer* k. *Therefore* $\mathbf{q}$ *contains the symbol 'zero'* $2p - 1$ *times and any nonzero symbol* $p - 1$ *times in one period.*

The last property in Lemma 1 can be seen very easily when we write the sequence $\mathbf{q}$ as an array of size $p \times p$:

$$\mathbf{q} = \begin{bmatrix} q(0) & q(1) & \cdots & q(p-1) \\ q(p) & q(p+1) & \cdots & q(2p-1) \\ q(2p) & q(2p+1) & \cdots & q(3p-1) \\ \vdots & \vdots & \ddots & \vdots \\ q((p-1)p) & q((p-1)p+1) & \cdots & q(p^2-1) \end{bmatrix} \tag{3}$$

The third item of Lemma 1 implies that every column (except for the left-most one) is balanced. We will present our first theorem, which is in fact a corollary to both Theorems 2 and 3.

Theorem 1: Assume that $\mathbf{q}$ *is a* p*-ary Fermat-quotient sequence of period* p^2.

1) $\mathbf{q}$ *is perfect.*
2) *The family of sequences*

$$\mathcal{F}(\mathbf{q}) = \{m \cdot \mathbf{q} | m = 1, 2, \ldots, p-1\} \tag{4}$$

is completely optimal, where $m \cdot \mathbf{q} = \{mq(t) | t \in \mathbb{Z}\}$ *is obtained by multiplying the constant* m *to every component of* $\mathbf{q}$.

Now we would like to focus on the following sequences of differences to identify the perfectness and find some essential properties.

Definition 3: Let τ *be an integer with* $1 \le \tau < p^2$. *We define a difference sequence* $\mathbf{d}_{\mathbf{s},\tau} = \{d_{\mathbf{s},\tau}(t) | t \in \mathbb{Z}\}$ *of a* p*-ary sequence* $\mathbf{s}$ *of period* p^2 *by*

$$d_{\mathbf{s},\tau}(t) \equiv s(t + \tau) - s(t) \pmod p.$$

We note that the sequence $\mathbf{d}_{\mathbf{s},\tau}$ has also period p^2. So we may write one period of a difference sequence [44] $\mathbf{d}_{\mathbf{s},\tau}$ of a p-ary sequence $\mathbf{s}$ of period p^2 as a $p \times p$ array as follows:

$$\mathbf{d}_{\mathbf{s},\tau} = \begin{bmatrix} d_{\mathbf{s},\tau}(0) & d_{\mathbf{s},\tau}(1) & \cdots & d_{\mathbf{s},\tau}(p-1) \\ d_{\mathbf{s},\tau}(p) & d_{\mathbf{s},\tau}(p+1) & \cdots & d_{\mathbf{s},\tau}(2p-1) \\ \vdots & \vdots & \ddots & \vdots \\ d_{\mathbf{s},\tau}((p-1)p) & d_{\mathbf{s},\tau}((p-1)p+1) & \cdots & d_{\mathbf{s},\tau}(p^2-1) \end{bmatrix}. \tag{5}$$

We observe that the sequence $\mathbf{s}$ is perfect if its difference sequence $\mathbf{d}_{\mathbf{s},\tau}$ is balanced for all $\tau = 1, 2, \ldots, p^2 - 1$. We also found that not only all their difference sequences are balanced in one period p^2, but also they could be balanced in every row or column when they are written as $p \times p$ arrays.

Definition 4: We say that a p*-ary sequence* $\mathbf{s}$ *of period* p^2 *has 'balanced difference sequences' if every difference sequence* $\mathbf{d}_{\mathbf{s},\tau}$ *is balanced for* $\tau = 1, 2, \ldots, p^2 - 1$.

We say that it has 'RC-balanced difference sequences' if, in the $p \times p$ *array representation of* $\mathbf{d}_{\mathbf{s},\tau}$ *as shown in* (5)*, every row is balanced for* $\tau = p, 2p, \ldots, (p-1)p$ *and every column is balanced for* $\tau \not\equiv 0 \pmod p$.

Note that if $\mathbf{s}$ has RC-balanced difference sequences then it has balanced difference sequences, but not conversely. The first item of Theorem 1 is essentially a corollary of the following theorem, whose proof will be covered by the discussions in Section III.

Theorem 2: The Fermat-quotient sequence has RC-balanced differece sequences.

We will characterize some transformations which preserve the perfectness of p-ary sequences of period p^2. These have been mentioned and even proved earlier [25], [35]. Here, we will consider preserving RC-balanced differences. Preserving the RC-balanced differences implies preserving the perfectness, but not conversely in general.

Lemma 2: Let $\mathbf{s} = \{s(t) | t \in \mathbb{Z}\}$ *be a* p*-ary sequence of period* p^2. *If* $\mathbf{s}$ *has RC-balanced difference sequences, then so do all the resulting sequences of the following transformations. Hence, they are also perfect.*

1) *(Constant Multiples)* $m \cdot \mathbf{s} = \{ms(t) | t \in \mathbb{Z}\}$ *for* $m \not\equiv 0 \pmod p$.
2) *(Constant Column Additions) For any* $0 \le j < p$, $\mathcal{A}_j(\mathbf{s})$ *is the sequence obtained from* $\mathbf{s}$ *by adding a constant* $1 \pmod p$ *to all the elements in the* j*-th column of* $\mathbf{s}$ *in the* $p \times p$ *array representation.*
3) *(Column Permutation)* $\mathcal{P}_\sigma(\mathbf{s})$ *is the sequence obtained from* $\mathbf{s}$ *by permuting the order of columns of* $\mathbf{s}$ *in the* $p \times p$ *array representation according to* σ, *where* σ *denotes a permutation in* p *symbols.*

Proof:

1) Let $\mathbf{s}' = m \cdot \mathbf{s}$. Then $\mathbf{d}_{\mathbf{s}',\tau} = m \cdot \mathbf{d}_{\mathbf{s},\tau}$ for all τ.
2) Let $\mathbf{s}' = \mathcal{A}_j(\mathbf{s})$. When $\tau \equiv 0 \pmod p$, the difference $s'(t+\tau) - s'(t)$ for $t = 0, 1, \ldots, p^2 - 1$ are the difference between the entries in a column of the $p \times p$ array. Therefore, $\mathbf{d}_{\mathbf{s}',\tau} = \mathbf{d}_{\mathbf{s},\tau}$.
   When $\tau \not\equiv 0 \pmod p$, for $t = 0, 1, \ldots, p^2 - 1$,
   $$s'(t + \tau) - s'(t) = \begin{cases} (s(t+\tau) + 1) - s(t) & t + \tau \equiv j \pmod{p^2} \\ s(t+\tau) - (s(t) + 1) & t \equiv j \pmod{p^2} \\ s(t+\tau) - s(t) & \text{otherwise} \end{cases}$$
   Therefore, $\mathbf{d}_{\mathbf{s}',\tau} = \mathcal{A}_j^{p-1}\mathcal{A}_{j-\tau}(\mathbf{d}_{\mathbf{s},\tau})$.
3) Observe that it is enough to show that RC-balancedness is preserved for $\sigma = (ab)$, the transposition of a-th and b-th columns. Let $\mathbf{s}' = \mathcal{P}_\sigma(\mathbf{s})$. Since $\mathbf{s}$ has RC-balanced difference sequences, $\mathbf{d}_{\mathbf{s},\tau}$ is row-balanced for $\tau \equiv 0 \pmod p$ and column-balanced for $\tau \not\equiv 0 \pmod p$ in its $p \times p$ array representation.
   For $\tau \equiv 0 \pmod p$, it is easy to see that
   $$\mathbf{d}_{\mathbf{s}',\tau} = \mathcal{P}_\sigma(\mathbf{d}_{\mathbf{s},\tau}).$$
   Therefore, row-balancedness is preserved.

TABLE I
EXAMPLE OF OPTIMAL FAMILIES FROM THE FERMAT-QUOTIENT SEQUENCE FOR $p = 5$

Family	$m = 1$	$m = 2$	$m = 3$	$m = 4$
$\mathcal{F}(\mathbf{q})$	$\begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 & 2 & 2 \\ 0 & 3 & 0 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \\ 0 & 4 & 3 & 0 & 3 \\ 0 & 2 & 2 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 4 & 3 & 3 \\ 0 & 2 & 0 & 2 & 1 \\ 0 & 4 & 1 & 1 & 4 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 3 & 3 & 4 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 2 & 4 & 4 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 2 & 3 & 3 & 2 \\ 0 & 3 & 1 & 0 & 1 \\ 0 & 4 & 4 & 2 & 0 \end{bmatrix}$
	$\mathbf{a}_1 = (0, 0, 0, 0, 0)$	$\mathbf{a}_2 = (0, 0, 1, 0, 0)$	$\mathbf{a}_3 = (2, 0, 0, 0, 1)$	$\mathbf{a}_4 = (0, 1, 2, 3, 4)$
$\mathcal{F}_A(\mathbf{q})$	$\begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 3 & 2 & 2 \\ 0 & 3 & 2 & 3 & 4 \\ 0 & 1 & 1 & 4 & 1 \\ 0 & 4 & 0 & 0 & 3 \\ 0 & 2 & 4 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 4 & 3 & 1 \\ 1 & 2 & 0 & 2 & 4 \\ 1 & 4 & 1 & 1 & 2 \\ 1 & 1 & 2 & 0 & 0 \\ 1 & 3 & 3 & 4 & 3 \end{bmatrix}$	$\begin{bmatrix} 0 & 4 & 0 & 1 & 0 \\ 0 & 0 & 3 & 3 & 4 \\ 0 & 1 & 1 & 0 & 3 \\ 0 & 2 & 4 & 2 & 2 \\ 0 & 3 & 2 & 4 & 1 \end{bmatrix}$

For $\tau \not\equiv 0 \pmod{p}$, it is not difficult to see that any column of $\mathbf{d}_{\mathbf{s}',\tau}$ is a column of $\mathbf{d}_{\mathbf{s},\tau'}$ for some $\tau' \not\equiv 0 \pmod{p}$. Therefore, column-balancedness is preserved. ■

We would like to recall that the family in Theorem 1 is obtained by applying all possible constant multiplications (First item of Lemma 2). Now, we consider the second transformation of Lemma 2. We denote:

$$\mathcal{A}^{\mathbf{a}} = \prod_{j=0}^{p-1} \mathcal{A}_j^{a(j)},$$

where $\mathbf{a} = \{a(t) | t \in \mathbb{Z}\}$ is an integer sequence of period p. Then, the transform $\mathcal{A}^{\mathbf{a}}(\mathbf{s})$ of $\mathbf{s}$ becomes the following:

$$\mathcal{A}^{\mathbf{a}}(\mathbf{s}) = \{s(t) + a(t) \pmod{p} | t \in \mathbb{Z}\}.$$

The following theorem is a generalized version of the family in Theorem 1 including the Constant Column Additions as well as the Constant Multiples. In fact, the second item of Theorem 1 is a corollary to the following theorem, whose proof will be covered by the discussions in Section III.

Theorem 3: Let $\mathbf{a}_m$ *be* $p - 1$ *integer sequences of period* p *for* $m = 1, 2, \ldots, p - 1$, *not necessarily all distinct. We construct a family of sequences of size* $p - 1$ *from the* p*-ary Fermat-quotient sequence* $\mathbf{q}$ *of period* p^2 *using* $\mathbf{a}_m$ *as*

$$\mathcal{F}_A(\mathbf{q}) = \{m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{q}) | m = 1, 2, ..., p - 1\}. \tag{6}$$

Then, the family $\mathcal{F}_A(\mathbf{q})$ *is completely optimal.*

Example 1: Table I *shows optimal families from* Theorems 1 *and* 3 *for the case* $p = 5$. *Note that* $\mathcal{F}_A(\mathbf{q}) = \{m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{q}) | 1 \le m < p\}$ *in the second row is also an optimal family with* $\mathbf{a}_1 = (0, 0, 0, 0, 0), \mathbf{a}_2 = (0, 0, 1, 0, 0), \mathbf{a}_3 = (2, 0, 0, 0, 1)$, *and* $\mathbf{a}_4 = (0, 1, 2, 3, 4)$.

Remark 2: It is quite surprising that any pair from $\mathcal{F}_A(\mathbf{q})$ *is completely optimal, considering that they could be distinct only in the constant multiplication. That is, Theorem 3 works even if the integer sequences* $\mathbf{a}_m$ *are all the same. We have checked the other direction by computer for* $p = 7$*: the cross-correlation of* $m \cdot \mathcal{A}^{\mathbf{a}}(\mathbf{q})$ *and* $m \cdot \mathcal{A}^{\mathbf{b}}(\mathbf{q})$ *for all possible different pairs* $(\mathbf{a}, \mathbf{b})$, *with the same constant* $m \not\equiv 0 \pmod{7}$. *It turned out that the pairs never be optimal.*

Remark 3: It is well-known in [17] and [25] *that the* p*-ary Frank-Zadoff sequence of period* p^2 *is perfect for every odd prime* p. *It has been first defined in the middle of 1950's, though the papers have appeared in 1961 and 1962. We denote the sequence as* $\mathbf{z} = \{z(t) | t \in \mathbb{Z}\}$ *in this paper.*

The structure of the Frank-Zadoff sequence can be seen when we write its one period as a $p \times p$ *array, where the indices* t *of* $z(t)$ *runs the first row from left to right, and then the second row, etc, which is the same as that in* (3). *Such a* $p \times p$ *array of* $\mathbf{z}$ *is the result of mod* p *reduction of the following:*

$$\begin{bmatrix} 1 & 2 & 3 & \cdots & p \\ 2 & 4 & 6 & \cdots & 2p \\ 3 & 6 & 9 & \cdots & 3p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p & 2p & 3p & \cdots & p^2 \end{bmatrix} \tag{7}$$

We note that Theorem 1 *will work if the sequence is replaced with the Frank-Zadoff sequence, which is the well-known results from many others* [17], [25], [51].

Similar to the last item of Lemma 1, for the p-ary Frank-Zadoff sequence $\mathbf{z} = \{z(t) | t \in \mathbb{Z}\}$ of period p^2, we have

$$z(t + kp) \equiv z(t) + k(t + 1) \pmod{p}, \tag{8}$$

for any integer $t \not\equiv 0 \pmod{p}$ and any integer k. It is obvious from this, as well as from the array structure of (7), that all the columns and rows are balanced except for the right-most column and the bottom row.

It turned out that Theorem 2 works if the sequence is replaced with the Frank-Zadoff sequence. That is, all its difference sequences are RC-balanced. We omit the proof since it is quite straightforward. Now, it is not too much surprising that Theorem 3 also works if the sequence is replaced with the Frank-Zadoff sequence. We will eventually prove this and discuss a lot more in general in the next section.

III. GENERAL APPROACH FOR OPTIMAL FAMILY

Recall that we construct optimal families of the form $m \cdot \mathbf{s}$ in Theorem 1 and of the form $m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{s})$ in Theorem 3, when $\mathbf{s}$ is the Fermat-quotient sequence (or the Frank-Zadoff sequence, which will soon be proved). In this section, we will investigate some similar construction of optimal families including the third item in Lemma 2. We hope that, when $\mathbf{s}$ is a p-ary perfect sequence of period p^2, some set of sequences given by

$$\mathcal{F}_P(\mathbf{s}) = \{m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathcal{P}_\sigma(\mathbf{s})) | m = 1, 2, \ldots, p - 1\} \tag{9}$$

$$\begin{aligned}\mathbf{s} &= \begin{bmatrix} s(0) & s(1) & \cdots & s(p-1) \\ s(0)+g(0) & s(1)+g(1) & \cdots & s(p-1)+g(p-1) \\ s(0)+2g(0) & s(1)+2g(1) & \cdots & s(p-1)+2g(p-1) \\ \vdots & \vdots & \ddots & \vdots \\ s(0)+(p-1)g(0) & s(1)+(p-1)g(1) & \cdots & s(p-1)+(p-1)g(p-1) \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} [s(0) \quad s(1) \quad \cdots \quad s(p-1)] + \begin{bmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{bmatrix} [g(0) \quad g(1) \quad \cdots \quad g(p-1)] \\ &\triangleq \underline{\mathbf{1}}^T \underline{\mathbf{s}} + \underline{\delta}^T \underline{\mathbf{g}}, \end{aligned} \tag{11}$$

is an optimal family for some $\mathbf{a}_m$ and σ. This construction does not increase the size of the optimal family, but this will give much more general description of constructing optimal families from a given perfect sequence. It turned out that we can find the Frank-Zadoff sequence in the family $\mathcal{F}_P(\mathbf{s})$ when we substitute $\mathbf{s}$ for the Fermat-quotient sequence in (9), or vice versa.

It turned out that not every σ results in an optimal family in (9). It is obvious that the following two cases work and in fact it is implicitly mentioned in [35]:

1) Taking a cyclic shift on the order of the columns in the $p \times p$ array.
2) Decimating the order of the columns in the $p \times p$ array.

It is not difficult but tedious to prove that (1) taking a cyclic shift on a sequence itself is the same as some combination of taking a cyclic shift on the order of columns and column-rotations on its array structure, and (2) decimating a sequence itself is the same as some combination of decimating the order of columns and column-rotations on its array structure. Here, a column-rotation is to rotate a column vertically in the array structure.

In this section, we will focus on the p-ary perfect sequences of period p^2 which have RC-balanced difference sequences. When we write the difference sequence in a $p \times p$ array, either every row is balanced or every column is balanced. For such a sequence, there are p^2-1 difference sequences, and we will focus on the difference sequence $\mathbf{d}_{\mathbf{s},p}$ at $\tau = p$ and we will see if it has period p. If $\mathbf{d}_{\mathbf{s},p}$ has period p, then the sequence $\mathbf{s}$ can be uniquely determined from $s(0), s(1), \ldots, s(p-1)$ and $d_{\mathbf{s},p}(0), d_{\mathbf{s},p}(1), \ldots, d_{\mathbf{s},p}(p-1)$.

Definition 5: When a p-ary sequence $\mathbf{s} = \{s(t)|t \in \mathbb{Z}\}$ of period p^2 has a difference sequence $\mathbf{d}_{\mathbf{s},p}$ that has period p, then $\mathbf{d}_{\mathbf{s},p}$ is called a generator of $\mathbf{s}$. On the other hand, given any p-ary sequence $\mathbf{g} = \{g(t)|t \in \mathbb{Z}\}$ of period p, the set of all the p-ary sequences of period p^2 having $\mathbf{g}$ as their common generator is called the associated family of $\mathbf{g}$, denoted by $\mathcal{S}(\mathbf{g})$.

Remark 4: A sequence $\mathbf{s} = \{s(t)|t \in \mathbb{Z}\} \in \mathcal{S}(\mathbf{g})$ can be written as a $p \times p$ array by setting $t = pi + j$ in which the (i, j) entry is given by, for $i = 0, 1, ..., p-1$ and $j = 0, 1, ..., p-1$,

$$s(pi + j) = g(j)i + s(j). \tag{10}$$

This is shown in (11)*, as shown at the top of this page where $\underline{\mathbf{1}}^T$ is the constant column of 1's, $\underline{\delta}^T$ is the column of entries $0, 1, 2, ..., p-1$, and $\underline{\mathbf{s}}$ and $\underline{\mathbf{g}}$ are the row vectors of length p representing the first p terms of $\mathbf{s}$ and $\mathbf{g}$, respectively. Since there are p^p choices for $\underline{\mathbf{s}}$, the associated family of a given generator contains exactly p^p different sequences.*

Remark 5: From the third property of Fermat-quotient sequences in Lemma 1 *and* (10)*, it is obvious that Fermat-quotient sequences have a generator given as*

$$g(j) \equiv -j^{p-2} \pmod{p} \tag{12}$$

for all $j \in \mathbb{Z}_p$. Similarly, from (8) *and* (10)*, it is obvious that Frank-Zadoff sequences have a generator given as*

$$g(j) \equiv j + 1 \pmod{p} \tag{13}$$

for all $j \in \mathbb{Z}_p$.

The p^p different sequences in the associated family $\mathcal{S}(\mathbf{g})$ of a generator $\mathbf{g}$ are not all cyclically distinct. The following lemma counts the number of cyclically inequivalent classes in $\mathcal{S}(\mathbf{g})$ when $\mathbf{g}$ is not a constant sequence.

Lemma 3: Let $\mathbf{g}$ be a non-constant generator of period p. Then, the associated family $\mathcal{S}(\mathbf{g})$ has p^{p-1} cyclically inequivalent classes each of which has size p.

Proof: Consider any member $\mathbf{s} \in \mathcal{S}(\mathbf{g})$. Then, there exist p^2 cyclic shifts of $\mathbf{s}$ in general since $\mathbf{s}$ has period p^2. Consider its cyclic shift by τ. When $\tau \not\equiv 0 \pmod{p}$, we claim that this cyclic shift will not have the generator $\mathbf{g}$. In fact, its generator is a cyclic shift of $\mathbf{g}$ by τ, which is clearly different from $\mathbf{g}$, since $\mathbf{g}$ has no subperiod less than p. Therefore, any of them will not be in $\mathcal{S}(\mathbf{g})$. On the other hand, when $\tau \equiv 0 \pmod{p}$, that is, when $\tau = kp$, the cyclic shift of $\mathbf{s}$ by τ will share the same generator $\mathbf{g}$ with $\mathbf{s}$. There exist p of them for $k = 0, 1, ..., p-1$. ∎

Example 2: Let $\mathbf{g} = (0, 1, 2)$ as a vector of length $p = 3$. Then the following three members of $\mathcal{S}(\mathbf{g})$ are cyclically equivalent with each other:

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 2 \end{bmatrix}.$$

Remark 6: There are lots of p-ary sequences of period p^2 which do not have a generator. A p-ary sequence of period p^2 has a generator if its difference sequence $\mathbf{d}_{\mathbf{s},p}$ has period p. Not every p-ary sequence of period p^2 having a generator is perfect. Furthermore, the followings are completely

open: (1) every perfect sequence has a generator; (2) every perfect sequence with RC-balanced difference sequence has a generator. We do not have a proof of any of the above and we do not know a counterexample to any of the above either.

From Remark 6, there seems to be no relation between the fact that a sequence has a generator and those that a sequence is perfect. However, Fermat-quotient sequences and Frank-Zadoff sequences have generators with some special property, which we will characterize in the following definition. Here,

$$m \cdot \mathbf{g} = \{mg(t) \pmod p | t \in \mathbb{Z}\}.$$

Definition 6: A generator $\mathbf{g}$ *is a perfect generator if all the sequences* $\mathbf{s} \in \mathcal{S}(\mathbf{g})$ *are perfect. A generator* $\mathbf{g}$ *is an optimal generator if two sequences* $\mathbf{u} \in \mathcal{S}(m \cdot \mathbf{g})$ *and* $\mathbf{v} \in \mathcal{S}(n \cdot \mathbf{g})$ *form an optimal pair for any* $m \not\equiv n \pmod p$ *and* $m, n \not\equiv 0 \pmod p$.

By Definition 6, an optimal generator is a perfect generator, but not conversely. Example 3 shows a perfect generator that is not an optimal generator.

Example 3: Let $(0, 3, 2, 4, 1, \ldots)$ *be a generator* $\mathbf{g}$ *of period 5. Then, one example of* $\mathbf{s} \in \mathcal{S}(\mathbf{g})$ *is shown below.*

$$\mathbf{s} = \begin{bmatrix} 1 & 0 & 3 & 1 & 4 \\ 1 & 3 & 0 & 0 & 0 \\ 1 & 1 & 2 & 4 & 1 \\ 1 & 4 & 4 & 3 & 2 \\ 1 & 2 & 1 & 2 & 3 \end{bmatrix}$$

It is a perfect sequence and so is every member of $\mathcal{S}(\mathbf{g})$. *It is easy to find a non-optimal pair* $\mathbf{u} \in \mathcal{S}(\mathbf{g})$ *and* $\mathbf{v} \in \mathcal{S}(2 \cdot \mathbf{g})$. *One choice would be obtained by setting the first row of both sequences* $(0, 0, 0, 0, 0)$. *Therefore,* $\mathbf{g}$ *is not an optimal generator.*

On the other hand, we will show later in Lemma 6 *that the generators of the Fermat-quotient sequences and the Frank-Zadoff sequences are optimal generators.*

Theorem 4: Let $\mathbf{g}$ *be an optimal generator of period* p. *Then, picking up any one member from* $\mathcal{S}(m \cdot \mathbf{g})$ *for each* $m = 1, 2, \ldots, p-1$ *gives an optimal family* $\mathcal{F}_G(\mathbf{g})$ *of size* $p-1$, *where* $\mathcal{S}(m \cdot \mathbf{g})$ *is the associated family of the generator* $m \cdot \mathbf{g}$.

Here, the proof is obvious by the definition of an optimal generator. We would like to note the relation between two sequences $\mathbf{s}_m \in \mathcal{S}(m \cdot \mathbf{g})$ in the above theorem and $m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathcal{P}_\sigma(\mathbf{s}))$ in (9). One can select $\mathbf{a}_m$ and an optimal generator $\mathbf{g}$ so that they coincide with each other if σ results in an optimal family of the form (9). Therefore, in order to characterize those permutations σ, we only have to characterize optimal generators.

The following lemma is about the vector sum of a prime regular polygon used in the proof of Theorem 5. Its proof is implied by [48, Th. 1].

Lemma 4: Let p *be a prime and* $\mathbf{a} = \{a(i) | i \in \mathbb{Z}, a(i) \in \mathbb{Z}_p\}$ *be a* p*-ary sequence of period* p. *Then* $\mathbf{a}$ *is balanced if and only if*

$$\sum_{i=0}^{p-1} \omega^{a(i)} = 0.$$

The following theorem describes some properties of perfect generators. We recall that not every perfect sequence has a generator and that not every sequence with RC-balanced differences has a generator either. Here, a generator $\mathbf{g}$ is said to be balanced if its one period is a permutation of $\{0, 1, 2, \ldots, p-1\}$.

Theorem 5 (Perfect Generator Construction): The followings are equivalent:

1) $\mathbf{g}$ *is a perfect generator.*
2) $\mathbf{g}$ *is balanced, or equivalently, it is a permutation of* $\{0, 1, ..., p-1\}$.
3) *Every sequence* $\mathbf{s} \in \mathcal{S}(\mathbf{g})$ *has RC-balanced difference sequences.*

Proof: Recall that any sequence $\mathbf{s} \in \mathcal{S}(\mathbf{g})$ can be written as in (11).

1) $\rightarrow$ 2): The autocorrelation of $\mathbf{s} \in \mathcal{S}(\mathbf{g})$ at $\tau = p$ is given by

$$C(\mathbf{s}, p) = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{s(p(i+1)+j) - s(pi+j)} = p \sum_{j=0}^{p-1} \omega^{g(j)}.$$

From Lemma 4, it becomes zero if and only if $\mathbf{g}$ is balanced

2) $\rightarrow$ 3): Consider a sequence $\mathbf{s} \in \mathcal{S}(\mathbf{g})$ with a balanced $\mathbf{g}$ and its difference sequence $d_{\mathbf{s},\tau}$.
Case 1 ($\tau = kp \equiv 0 \ (mod\ p)$): The set of elements from i-th row of the array representation of $d_{\mathbf{s},kp}$ is given as

$$\begin{aligned} &\{s(p(i+k)+j) - s(pi+j) | j = 0, 1, \ldots, p-1\} \\ &= \{kg(j) | j = 0, 1, \ldots, p-1\}, \end{aligned}$$

which must be balanced since $k \not\equiv 0 \pmod p$ and $g(j)$ is balanced.
Case 2 ($\tau \not\equiv 0 \ (mod\ p)$): The element in i-row and j-th column of the array representation of $d_{\mathbf{s},\tau}$ is given as

$$\begin{aligned} &s(pi + j + \tau) - s(pi + j) \\ &= (s(j+\tau) - s(j)) - i(g(j+\tau) - g(j)). \end{aligned}$$

Therefore, the set of elements in j-th column (for $i = 0, 1, ..., p-1$) must be balanced since $g(j+\tau) \not\equiv g(j) \pmod p$ for any j.

3) $\rightarrow$ 1): Obvious by definition. ■

Remark 7: Note that the result of the construction in Theorem 5 *does not produce new perfect sequences. All the sequences in the associated family of the perfect generators from* Theorem 5 *are essentially the same as those obtained by Heimiller's generalization* [17]. *The sequences are also considered in* [31] *as bent functions, and are treated by Mow's unified construction* [41].

Next we determine the property of optimal generators. To do this, we have to use the periodic Hamming cross-correlation [33] of two p-ary sequences $\mathbf{u}$ and $\mathbf{v}$ of period p, denoted by $H(\mathbf{u}, \mathbf{v}, \tau)$, and defined as follows:

$$H(\mathbf{u}, \mathbf{v}, \tau) = \sum_{t=0}^{p-1} h(u(t+\tau), v(t)), \quad \tau = 0, 1, 2, \ldots, p-1,$$

where $h(x, y) = 1$ if $x = y$ and $h(x, y) = 0$ otherwise. Note that $H(\mathbf{u}, \mathbf{v}, \tau) = 1$ is equivalent to the existence of a unique solution to $u(t + \tau) \equiv v(t) \pmod p$.

Theorem 6: A generator $\mathbf{g}$ *is an optimal generator if*

$$H(m \cdot \mathbf{g}, n \cdot \mathbf{g}, \tau) = 1$$

for all $\tau = 0, 1, 2, \ldots, p-1$, *and for any* $m, n \not\equiv 0 \pmod p$ *and* $m \not\equiv n \pmod p$. *Moreover, any family given by* Theorem 4 *from the optimal generator above is completely optimal.*

Proof: (Proof of Perfectness) Assume that $\mathbf{g}$ satisfies $H(m \cdot \mathbf{g}, n \cdot \mathbf{g}, \tau) = 1$ for all $\tau = 0, 1, 2, \ldots, p-1$, and for any $m, n \not\equiv 0 \pmod p$ and $m \not\equiv n \pmod p$. Suppose that $\mathbf{g}$ is not balanced, that is, $g(a) \equiv g(a + b) \pmod p$ for some $0 \le a < p$ and $1 \le b < p$. Observe that $g(a) \not\equiv 0 \pmod p$, since otherwise, $H \ge 2$ for all $m \ne n$ for $\tau = b$. Note that $H(m \cdot \mathbf{g}, n \cdot \mathbf{g}, \tau) = 1$ for any τ and any $m \ne n$ implies that there exists a unique solution t in $0 \le t < p$ to the equation $mg(t+\tau) \equiv ng(t) \pmod p$ for any given $m \ne n$ and τ. Note also that there exists a unique z in $0 \le z < p$ such that $g(z) = 0$, since the equation $mg(t) \equiv ng(t) \pmod p$ for the case of $\tau = 0$ must also have a unique solution. Therefore, $a \not\equiv z \pmod p$ and $a + b \not\equiv z \pmod p$.

Denote by t_m the unique solution to the equation $mg(t + b) \equiv g(t) \pmod p$, for each $m = 2, 3, ..., p-1$. Observe that $t_m \not\equiv z \pmod p$ since $t_m \equiv z \pmod p$ implies $g(t_m) = 0 = g(z)$ and hence $H(m \cdot \mathbf{g}, \mathbf{g}, \tau = b) \ge 2$. Similarly, we have $t_m \not\equiv z - b \pmod p$ and $t_m \not\equiv a \pmod p$. Since the three elements z, a, $z - b$ must all be distinct mod p, we have

$$|\{t_m | m = 2, 3, ..., p-1\}| \le p - 3. \tag{14}$$

On the other hand, $mg(t_m + b) \equiv g(t_m) \pmod p$ implies that $m \equiv \frac{g(t_m)}{g(t_m+b)} \pmod p$. This shows that $t_2, t_3, \ldots, t_{p-1}$ are all distinct, which is a desired contradiction to (14). Therefore $\mathbf{g}$ must contain any symbol at most once. Since it has length p, it must be balanced.

(Proof of optimality) From Lemma 2, $m \cdot \mathbf{g}$ is also a perfect generator for all $m \not\equiv 0 \pmod p$. Let $\mathbf{s} \in \mathcal{S}(\mathbf{g})$, $\mathbf{u} \in \mathcal{S}(m \cdot \mathbf{g})$ and $\mathbf{v} \in \mathcal{S}(n \cdot \mathbf{g})$. It is easy to see that there exist integer sequences $\mathbf{a}$ and $\mathbf{b}$ satisfying $\mathbf{u} = m\mathcal{A}^{\mathbf{a}}(\mathbf{s})$ and $\mathbf{v} = n\mathcal{A}^{\mathbf{a}}(\mathbf{s})$. Therefore,

$$u(t) = m(s(t) + a(t)) \text{ and } v(t) = n(s(t) + b(t)),$$

for all t. Since $\mathbf{s} \in \mathcal{S}(\mathbf{g})$, it must be of the form

$$s(t) = s(pi + j) = s(j) + ig(j),$$

for all $t = pi + j$. Therefore, the cross-correlation of two sequences $\mathbf{u}$ and $\mathbf{v}$ can be computed as

$$\begin{aligned}
&C(\mathbf{u}, \mathbf{v}, \tau) \\
&= C(m \cdot \mathcal{A}^{\mathbf{a}}(\mathbf{s}), n \cdot \mathcal{A}^{\mathbf{b}}(\mathbf{s}), \tau) \\
&= \sum_{t=0}^{p^2-1} \omega^{ms(t+\tau) - ns(t) + ma(t+\tau) - nb(t)} \\
&= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{ms(pi+j+\tau) - ns(pi+j) + ma(pi+j+\tau) - nb(pi+j)} \\
&= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{ms(j+\tau) + mig(j+\tau) - ns(j) - nig(j) + ma(j+\tau) - nb(j)} \\
&= \sum_{j=0}^{p-1} \omega^{ms(j+\tau) - ns(j) + ma(j+\tau) - nb(j)} \sum_{i=0}^{p-1} \omega^{i\{mg(j+\tau) - ng(j)\}}
\end{aligned} \tag{15}$$

Now, the inner sum of (15) is not zero and have magnitude p if and only if $mg(j + \tau) \equiv ng(j) \pmod p$. But this relation must be satisfied for exactly one value j_0 of j since the number of solutions j is the Hamming correlation value of $m \cdot \mathbf{g}$ and $n \cdot \mathbf{g}$ at the shift τ. Thus, the inner sum vanished except for $j = j_0$, and the outer-sum becomes a single term for $j = j_0$. That is,

$$|C(\mathbf{u}, \mathbf{v}, \tau)| = p$$

for all $\tau = 0, 1, 2, \ldots, p-1$, and for any $m, n \not\equiv 0 \pmod p$ and $m \not\equiv n \pmod p$. Therefore $\mathbf{g}$ is an optimal generator. ∎

Remark 8: Theorem 6 *gives a sufficient condition on a generator to be optimal. We do not know whether there exists an optimal generator without such condition. We confirmed that every optimal generator satisfies the condition in* Theorem 6 *for* $p \le 13$ *using computers.*

Theorem 7 gives some transformations that preserve the optimality of a generator.

Theorem 7: If $\mathbf{g} = \{g(t) | t \in \mathbb{Z}\}$ *is an optimal generator of period p, then the following generators are also optimal generators.*

1) *(Cyclic Shifts)* $\mathcal{T}_\tau(\mathbf{g}) = \{g(t + \tau) | t \in \mathbb{Z}\}$ *for any integer* τ.
2) *(Constant Multiples)* $m \cdot \mathbf{g}$ *for* $m \not\equiv 0 \pmod p$.
3) *(Decimations)* $\mathcal{D}_d(\mathbf{g}) = \{g(dt) | t \in \mathbb{Z}\}$ *for* $d \not\equiv 0 \pmod p$.

Proof:

1) If $\mathbf{u}$ and $\mathbf{v}$ form an optimal pair of sequences, then so do $\mathcal{T}_\tau(\mathbf{u})$ and $\mathcal{T}_\tau(\mathbf{v})$ for any integer τ, and vice versa. Here, we use the operator $\mathcal{T}_\tau(\cdot)$ to work on the sequence of period p^2 as a cyclic shift by τ. From (11), we have

$$\begin{aligned}
&\mathbf{u} \in \mathcal{S}(m \cdot \mathcal{T}_\tau(\mathbf{g})) \\
\leftrightarrow\ &\mathbf{u} = \underline{\mathbf{1}}^T \underline{\mathbf{u}} + m \cdot \underline{\delta}^T \mathcal{T}_\tau(\underline{\mathbf{g}}) \\
&= \underline{\mathbf{1}}^T \underline{\mathbf{u}} + \mathcal{T}_\tau(m \cdot \underline{\delta}^T \underline{\mathbf{g}}) \\
\leftrightarrow\ &\mathcal{T}_{-\tau}(\mathbf{u}) = \underline{\mathbf{1}}^T \underline{\mathcal{T}_{-\tau}(\mathbf{u})} + m \cdot \underline{\delta}^T \underline{\mathbf{g}} \in \mathcal{S}(m \cdot \mathbf{g}).
\end{aligned}$$

   Assume that $m, n \not\equiv 0 \pmod p$ and $m \not\equiv n \pmod p$. If $\mathbf{u} \in \mathcal{S}(m \cdot \mathcal{T}_\tau(\mathbf{g}))$ and $\mathbf{v} \in \mathcal{S}(n \cdot \mathcal{T}_\tau(\mathbf{g}))$, then $\mathcal{T}_{-\tau}(\mathbf{u}) \in \mathcal{S}(m \cdot (\mathbf{g}))$ and $\mathcal{T}_{-\tau}(\mathbf{v}) \in \mathcal{S}(n \cdot (\mathbf{g}))$, and hence, they form an optimal pair, and so do $\mathbf{u} = \mathcal{T}_\tau(\mathcal{T}_{-\tau}(\mathbf{u}))$ and $\mathbf{v}$.
2) Obvious.
3) We may proceed similarly as the first item of the above, using the fact that $\mathbf{u}$ and $\mathbf{v}$ form an optimal pair of sequences if and only if so do $\mathcal{D}_d(\mathbf{u})$ and $\mathcal{D}_d(\mathbf{v})$ for $d \not\equiv 0 \pmod p$ [35]. Here, we use the operator $\mathcal{D}_d(\cdot)$ to work on the sequence of period p^2 as a decimation by d. ∎

Now we focus on the balanced generators $\mathbf{g}$ of period p. Then, the first and second transformations in Theorem 7 on a balanced $\mathbf{g}$ never coincide. Therefore, one can find $p(p-1)$ different optimal generators from a given optimal generator. On the other hand, things are more complicated when we include the third transformation into the picture. It turned out that some decimations of a balanced $\mathbf{g}$ can also be obtained by applying some combination of the first and second transformations, while some other decimations of $\mathbf{g}$ cannot be obtained in such a way. To discuss this property further, we need the following definition of "equivalence" excluding the third transformation (decimations) in Theorem 7:

Definition 7: Two p-ary generators of the same period p are said to be equivalent if one can be obtained from another by applying some combination of the first and second transformations in Theorem 7.

Consider the set of all the balanced generators of period p. It is exactly the same as the set of all the permutations on p symbols. We will consider the equivalence relation on this set which is given in Definition 7. We denote by Class($\mathbf{g}$) the equivalence class containing the generator $\mathbf{g}$.

Lemma 5: Consider the set of all the balanced generators $\mathbf{g}$ *of period p, and its partition into equivalence classes.*

1) *For any* $\mathbf{g}$*, there exists a generator* $\mathbf{h} \in$ Class($\mathbf{g}$) *such that* $h(0) = 0$ *and* $h(1) = 1$.
2) *These are equivalent:*
   a) *There exists* $\mathbf{h} \in$ Class($\mathbf{g}$) *that satisfies* $h(ab) \equiv h(a)h(b) \pmod p$ *for any integers a and b.*
   b) *Any decimation of* $\mathbf{g}$ *belongs to* Class($\mathbf{g}$).
   c) *Any decimation of* $\mathbf{g}'$ *belongs to* Class($\mathbf{g}$) *for any* $\mathbf{g}' \in$ Class($\mathbf{g}$).

Proof:

1) There exists a unique value of t that satisfies $g(t) = 0$. Since g is balanced, $g(t+1) \not\equiv 0 \pmod p$. Let $\mathbf{h} = g(t+1)^{-1}\mathcal{T}_t(\mathbf{g})$. Obviously, $\mathbf{h} \in$ Class($\mathbf{g}$) and $h(0) = 0, h(1) = 1$
2) a) $\rightarrow$ b): Obviously, a generator $\mathbf{h}$ satisfying $h(ab) \equiv h(a)h(b)$ for all a and b has $h(0) = 0$ and $h(1) = 1$. Note that $\mathcal{D}_d(\mathbf{h}) = \{h(dt) | t = 0, 1, \ldots, p-1\} = h(d)\mathbf{h}$, so any decimation of $\mathbf{h}$ is equivalent with $\mathbf{h}$.
   Now, let $\mathbf{g} = m \cdot \mathcal{T}_\tau(\mathbf{h})$ with such $\mathbf{h} \in$ Class($\mathbf{g}$). From the relation, $\mathcal{D}_d(\mathbf{g}) = \mathcal{D}_d(m \cdot \mathcal{T}_\tau(\mathbf{h})) = \{mh(dt + d\tau)\} = m \cdot \mathcal{T}_{d\tau}\mathcal{D}_d(\mathbf{h})$, so $\mathcal{D}_d(\mathbf{g}) \in$ Class($\mathbf{h}$) = Class($\mathbf{g}$) for any $d \not\equiv 0 \pmod p$.
   b) $\rightarrow$ c): We can find the equivalent generator $\mathbf{g}' = m \cdot \mathcal{T}_\tau(\mathbf{g})$. Since $\mathcal{D}_d(\mathbf{g}') = m \cdot \mathcal{T}_{d\tau}\mathcal{D}_d(\mathbf{g})$, any decimations of $\mathbf{g}'$ also belongs to Class($\mathbf{g}'$) = Class($\mathbf{g}$).
   c) $\rightarrow$ a): From Lemma 5-1), we can find $\mathbf{h}$ that any decimation of $\mathbf{h}$ belongs to Class($\mathbf{g}$) and $h(0) = 0, h(1) = 1$. Let $\mathcal{D}_d(\mathbf{h}) = m \cdot \mathcal{T}_\tau(\mathbf{h})$, so $h(dt) = mh(t + \tau)$ for all t with some $m \not\equiv 0 \pmod p$ and some integer τ. In this case τ must be congruent to 0 since $mh(0 + \tau) = h(0) = 0$. So $h(dt) = mh(t)$ for all t with some m determined by d. We denote such m as m_d. The case with $d = 0$ also satisfies the equation with $m_0 \equiv 0 \pmod p$.

   We have shown that $h(dt) = m_d h(t)$ for any d and t. So, it is also true that $h(dt) = m_t h(d)$ for any d and t, and it indicates $m_t h(d) = m_d h(t)$ for any d and t. Obviously, $m_1 = 1$, so the equation becomes $m_t = h(t)$ putting $d = 1$. So $h(dt) = m_t h(d)$ becomes $h(dt) = h(d)h(t)$ for any d and t. ■

Theorem 8: Let $\mathbf{g}$ *be a balanced p-ary generator of period p. If* $\mathbf{g}$ *is equivalent* (*in the sense of* Definition 7) *with all its decimations, then it satisfies the Hamming correlation property in* Theorem 6. *Hence, it is an optimal generator.*

Proof: Assume that $\mathbf{g}$ is equivalent with all its decimations. From the second item of Lemma 5, this implies the existence of a generator $\mathbf{h} \in$ Class($\mathbf{g}$) such that $h(ab) \equiv h(a)h(b) \pmod p$ for all a and b. Now, claim that $\mathbf{h}$ satisfies the Hamming correlation property in Theorem 6. Then, it is obvious that so does $\mathbf{g}$.

To show the claim, we have to argue that the equation

$$mh(t+\tau) \equiv nh(t) \pmod p$$

has a unique solution $t \pmod p$ for all $\tau, m, n \not\equiv 0 \pmod p$ and $m \not\equiv n \pmod p$. The multiplicative property of $\mathbf{h}$ implies that $h(0) = 0$ and $h(1) = 1$.

When $\tau \equiv 0 \pmod p$, the equation becomes

$$mh(t) \equiv nh(t) \pmod p.$$

Therefore, $h(t) = 0$ and hence $t = 0$ is a solution, since otherwise we have $m \equiv n \pmod p$, and it is the only solution since $\mathbf{h}$ is balanced.

When $\tau \not\equiv 0 \pmod p$, since $t = 0$ can never be a solution, one can write

$$h(t+\tau) \equiv h(t)h\left(\frac{t+\tau}{t}\right),$$

or

$$h\left(\frac{t+\tau}{t}\right) \equiv \frac{h(t+\tau)}{h(t)} \equiv \frac{n}{m} \pmod p.$$

Since $\mathbf{h}$ is balanced in a period p, the above has a unique solution t. ■

Remark 9: It is open whether the converse of Theorem 8 *is true in general. We confirmed that this is true for* $p \leq 23$ *using computers.*

Lemma 6: The generator of Fermat-quotient sequences given by (Remark 5)

$$g(t) \equiv -t^{p-2} \pmod p, \quad t = 0, 1, 2, \ldots,$$

is an optimal generator. So is the generator of Frank-Zadoff sequences given by (Remark 5)

$$g(t) \equiv t + 1 \pmod p, \quad t = 0, 1, 2, \ldots.$$

Proof: Let $\mathbf{h} = \mathcal{D}_d(\mathbf{g})$. For the generator of Fermat-quotient sequences, we have $h(t) = g(dt) = -(dt)^{p-2} = -d^{p-2}g(t)$ for all t. Therefore, any decimation of $\mathbf{g}$ is a constant multiple of $\mathbf{g}$, and we are done by Theorem 8. For the generator of Frank-Zadoff sequence, similarly, we have $h(t) = g(dt) = dt + 1 = \mathcal{T}_{\frac{1-d}{d}}(dg(t))$ for all t. ■

We now present an algebraic construction for some important class of optimal generators, which satisfy the sufficient condition in Theorem 8. Let $\mathbf{g} = \{g(t) | t \in \mathbb{Z}\}$ be an

optimal generator that is balanced and any of its decimations is equivalent to itself in the sense of Definition 7. It can be uniquely determined if $g(0) = 0, g(1) = 1$ and the value $g(\alpha)$ is given for a primitive root α of p. Let $g(\alpha) = \beta$. Then, from the multiplicative property in the second item of Lemma 5, we have $g(\alpha^l) = \beta^l$ for any $l = 0, 1, 2, \ldots$. Since $\mathbf{g}$ is balanced, β must also be a primitive root of p.

Theorem 9 (Optimal Generator Construction): Let τ be any integer, m be an integer with $m \not\equiv 0 \pmod p$ and κ be an integer relatively prime to $p-1$. Then, the sequence $\mathbf{g}(p, \kappa, m, \tau) = \{g(t; p, \kappa, m, \tau) | t \in \mathbb{Z}\}$ defined as:

$$g(t; p, \kappa, m, \tau) \equiv m(t+\tau)^{\kappa} \pmod p, \tag{16}$$

is a perfect generator and is equivalent with its decimated sequences, and conversely. Hence, $\mathbf{g}(p, \kappa, m, \tau)$ is an optimal generator.

Proof: Observe that it is enough to prove the case $m = 1$ and $\tau = 0$ since any two generators having the same κ are equivalent, since

$$\mathbf{g}(p, \kappa, m, \tau) = m \cdot \mathbf{g}(p, \kappa, 1, \tau),$$

and

$$g(t; p, \kappa, 1, \tau) = g(t - \tau; p, \kappa, 1, 0), \quad \forall t.$$

Now, consider the generator given by

$$g(t; p, \kappa, 1, 0) \equiv t^{\kappa} \pmod p.$$

It is balanced since κ is relatively prime to $p-1$. Moreover, $g(ab) = g(a)g(b)$ for any a and b. The proof is now completed using the second item of Lemma 5.

To prove the converse, we note that $\mathbf{g}(p, \kappa, 1, 0)$ and $\mathbf{g}(p, \lambda, 1, 0)$ are inequivalent if $\kappa \not\equiv \lambda \pmod{p-1}$. So we can find $\varphi(p-1)$ inequivalent generators of period p varying κ of $\mathbf{g}(p, \kappa, 1, 0)$, where φ is the Euler's totient function. We already noted that if a p-ary perfect generator $\mathbf{g} = \{g(t) | t \in \mathbb{Z}\}$ with $g(0) = 0$, $g(1) = 1$ and all of its decimated sequences are equivalent with $\mathbf{g}$, then $g(t)$ has the multiplicative property in 2a) of Lemma 5 and so can be represented as $g(\alpha^l) = \beta^l$ for some primitive roots α and β of p. This indicates there are at most $\varphi(p-1)$ inequivalent generators each of which is balanced and equivalent with all of its decimations. ∎

Remark 10: Let m, n be integers with $m, n \not\equiv 0 \pmod p$. Let κ, λ be integers relatively prime to $p-1$ and τ, μ be any integers. Then, two optimal generators $\mathbf{g}(p, \kappa, m, \tau)$ and $\mathbf{g}(p, \lambda, n, \mu)$ are equivalent if and only if $\kappa \equiv \lambda \pmod{p-1}$. There are exactly $\varphi(p-1)$ inequivalent optimal generators of period p of the form given in Theorem 9*, where φ is the Euler's totient function. It is open whether there exists any other type of optimal generators. For $p \leq 13$, it is confirmed by computers that every optimal generator is given by* Theorem 9*.*

Remark 11: Observe that, from Remark 5*, the integer sequence $\mathbf{g}(p, p-2, p-1, 0)$ is the generator of p-ary Fermat-quotient sequence, and the integer sequence $\mathbf{g}(p, 1, 1, 1)$ is the generator of p-ary Frank-Zadoff sequence. Therefore, they are equivalent if and only if $p = 3$. We note that the optimality of these generators in* Lemma 6 *proves* Theorems 2 *and* 3*. Furthermore, note that we obtain an optimal family $\mathcal{F}_G(\mathbf{g_z})$ in* Theorem 4 *when we use the generator $\mathbf{g_z} = \mathbf{g}(p, 1, 1, 1)$ of a p-ary Frank-Zadoff sequence. This gives a proof of the assertion at the end of* Section II *that* Theorem 3 *works if the sequence is replaced with the Frank-Zadoff sequence. That is, one can arrange such that*

$$\mathcal{F}_G(\mathbf{g_z}) = \mathcal{F}_A(\mathbf{z})$$

where $\mathbf{z}$ is the p-ary Frank-Zadoff sequence of period p^2.

Remark 12: The $p \times p$ array structure of both Fermat-quotient sequences and Frank-Zadoff sequences gives a clue to how they are related. From the third property in Lemma 1 *and* (8)*, they differ only in two aspects: the generator and the first p terms. That is, for Fermat-quotient sequences $q(t) = q(ip + j)$,*

$$q(ip + j) \equiv g_q(j)i + q(j) \equiv -j^{p-2}i + q(j) \pmod p$$

and, for Frank-Zadoff sequences $z(t) = z(ip + j)$,

$$z(ip + j) \equiv g_z(j)i + z(j) \equiv (j+1)i + z(j) \pmod p$$

all for $i, j \in \mathbb{Z}_p$. This gives the following relation between $q(ip + j)$ and $z(ip + j)$:

Case 1: For $j \not\equiv 0 \pmod p$,

$$(-j)q(ip + j) \equiv i + (-j)q(j) \pmod p,$$

or

$$-j(j+1)q(ip + j) \equiv (j+1)i - j(j+1)q(j) \pmod p,$$

or

$$\begin{aligned} -j(j+1)q(ip + j) + j(j+1)q(j) + z(j) \\ \equiv (j+1)i + z(j) \equiv z(ip + j) \pmod p. \end{aligned}$$

Case 2: For $j \equiv 0 \pmod p$,

$$\begin{aligned} q(ip + j) &\equiv 0 \pmod p \quad \text{or} \\ q(ip + j) + i + 1 &\equiv i + 1 \equiv z(ip + j) \pmod p, \end{aligned}$$

which gives a conversion from Fermat-quotient sequences to Frank-Zadoff sequences.

IV. Numerical Results and Concluding Remarks

We have done some exhaustive computer search for optimal generators. The number of inequivalent optimal generators of period p is confirmed to be $\varphi(p-1)$ for $p \leq 13$. This implies that all the optimal generators of period $p \leq 13$ can be constructed from Theorem 9. The number of inequivalent optimal generators of period p with the Hamming correlation property of Theorem 6 is also confirmed to be $\varphi(p-1)$ for $p \leq 23$. These results support the following:

Conjecture 1: All the optimal generators can be constructed by Theorem 9*.*

In general, there are huge number of perfect generators but only a small portion of them are optimal generators. We observe that the number of perfect generators is $p!$ (Theorem 5) while the number of optimal generators from

TABLE II

LIST OF ALL THE INEQUIVALENT OPTIMAL GENERATORS FOR $p \leq 13$ AND THEIR REPRESENTATIONS OF THE FORM $\mathbf{g}[p, \kappa, 1, 0]$

p	optimal generators (representatives)	κ
3	{0,1,2} (FZ)	1
5	{0,1,2,3,4} (Z)	1
	{0,1,3,2,4} (F)	3
7	{0,1,2,3,4,5,6} (Z)	1
	{0,1,4,5,2,3,6} (F)	5
11	{0,1,2,3,4,5,6,7,8,9,10} (Z)	1
	{0,1,6,4,3,9,2,8,7,5,10} (F)	9
	{0,1,7,9,5,3,8,6,2,4,10}	7
	{0,1,8,5,9,4,7,2,6,3,10}	3
13	{0,1,2,3,4,5,6,7,8,9,10,11,12} (Z)	1
	{0,1,6,9,10,5,2,11,8,3,4,7,12}	5
	{0,1,7,9,10,8,11,2,5,3,4,6,12} (F)	11
	{0,1,11,3,4,8,7,6,5,9,10,2,12}	7

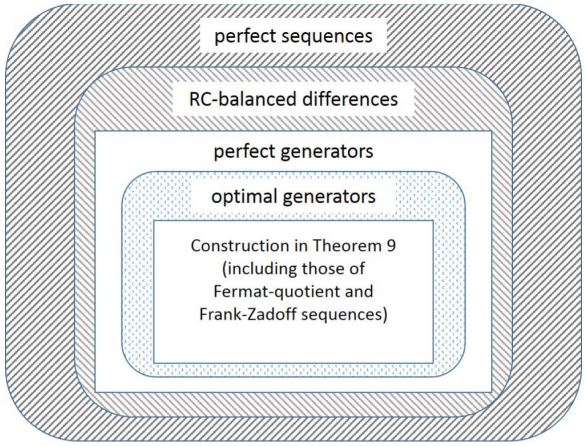

Fig. 1. Hierarchy of p-ary perfect sequences of period p^2.

Theorem 9 is $p(p-1)\varphi(p-1)$. Now, the number of inequivalent (in the sense of Definition 7) perfect generators of period p is $(p-2)!$. All the inequivalent optimal generators which are exhaustively found by computer are shown in Table II for $p \leq 13$, including their representations of the form $\mathbf{g}[p, \kappa, 1, 0]$. Here, (F) indicates that it is the generator of Fermat-quotient sequence and (Z) indicates that it is the generator of Frank-Zadoff sequence.

Figure 1 shows the hierarchy of p-ary perfect sequences of period p^2. A perfect sequence may or may not have RC-balanced difference sequences. A perfect sequence with RC-balanced differences may or may not have the perfect generator. The generator of a perfect sequence may or may not be an optimal generator. We have an example of perfect generator which is not an optimal generator (Example 3). The optimal generator of a perfect sequence, if it has an optimal generator, may or may not come from Theorem 9. It shows a brief summary of Theorems 5, 6, 8 and 9. The shaded or dotted area indicates that non-existence has not been proved yet and that no example is currently known either.

Mow [41] conjectured that the number of p-ary perfect sequences of period p^2 may not exceed $p!p^p$. The number of such sequences that can be generated by the perfect generators derived in Theorem 5 is exactly $p!p^p$. Therefore, if Mow's conjecture is true, then both of the shaded areas outside 'Perfect Generators' in Figure 1 will be empty. On the other hand, the truth of Conjecture 1 above implies that the inner dotted area becomes empty.

REFERENCES

[1] *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation (Release 12)*, document 3GPP TS 36.211 V12.3.0, 2014.

[2] *Global Positioning Systems Directorate Systems Engineering & Integration Interface Specification*, document IS-GPS-200G, 2012.

[3] R. H. Barker, "Group synchronization of binary digital systems," in *Communication Theory*, W. Jackson, Ed. London, U.K.: Academic, 1953, pp. 273–287.

[4] N. C. Beaulieu and D. J. Young, "Designing time-hopping ultrawide bandwidth receivers for multiuser interference environments," *Proc. IEEE*, vol. 97, no. 2, pp. 255–284, Feb. 2009.

[5] S. T. Blake and A. Z. Tirkel, "A construction for perfect periodic autocorrelation sequences," in *Sequences and Their Applications—SETA* (Lecture Notes Computer Science), vol. 8865. New York, NY, USA: Springer, Nov. 2014, pp. 104–108.

[6] M. Antweiler, "Polyphase Barker sequences," *Electron. Lett.*, vol. 25, no. 23, pp. 1577–1579, Nov. 1989.

[7] R. Chen and B. Cantrell, "Highly bandlimited radar signals," in *Proc. IEEE Radar Conf.*, Long Beach, CA, USA, Apr. 2002, pp. 220–226.

[8] Z. Chen, A. Ostafe, and A. Winterhof, "Structure of pseudorandom numbers derived from Fermat quotients," in *Proc. Workshop Arithmetic Finite Fields*, 2010, pp. 73–85.

[9] Z. Chen, "Trace representation and linear complexity of binary sequences derived from Fermat quotients," *Sci. China Inf. Sci.*, vol. 57, no. 11, pp. 1–10, Nov. 2014.

[10] Z. Chen, X. Du, and R. Marzouk. (2014). "Trace representation of pseudorandom binary sequences derived from Euler quotients." [Online]. Available: http://arxiv.org/abs/1408.2385

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

[12] J.-H. Chung and K. Yang, "A new class of balanced near-perfect nonlinear mappings and its application to sequence design," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1090–1097, Feb. 2013.

[13] H. Ebner, "Galileo overall architecture definition: SIS frequency characteristics," Tech. Rep. GALA-ASTR-DD-020, Sep. 2000.

[14] R. Ernvall and T. Metsänkylä, "On the p-divisibility of Fermat quotients," *Math. Comput.*, vol. 66, no. 219, pp. 1353–1365, 1997.

[15] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. Baldock, U.K.: Research Studies Press, 1996.

[16] R. L. Frank, "Polyphase codes with good nonperiodic correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-9, no. 1, pp. 43–45, Jan. 1963.

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

[18] R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: A combinatorial approach," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2408–2420, Oct. 2004.

[19] 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.

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

[21] S. W. Golomb and R. A. Scholtz, "Generalized Barker sequences," *IEEE Trans. Inf. Theory*, vol. IT-11, no. 4, pp. 533–537, Oct. 1965.

[22] S. W. Golomb, "Two-valued sequences with perfect periodic autocorrelation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 28, no. 2, pp. 383–386, Mar. 1992.

[23] D. Gomez and A. Winterhof, "Multiplicative character sums of Fermat quotients and pseudorandom sequences," *Periodica Math. Hungarica*, vol. 64, no. 2, pp. 161–168, 2012.

[24] G. Gong and H.-Y. Song, "Two-tuple balance of non-binary sequences with ideal two-level autocorrelation," *Discrete Appl. Math.*, vol. 154, no. 18, pp. 2590–2598, 2006.
[25] R. C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory*, vol. IT-7, no. 4, pp. 254–257, Oct. 1961.
[26] V. P. Ipatov, *Periodic Discrete Signals With Optimal Correlation Properties*. Moscow, Russia: Radio I Svyaz, 1992.
[27] J. W. Kang, Y. Whang, B. H. Ko, and K. S. Kim, "Generalized cross-correlation properties of Chu sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 438–444, Jan. 2012.
[28] D. S. Kim, H.-J. Chae, and H.-Y. Song, "A generalization of the family of p-ary decimated sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7614–7617, Nov. 2011.
[29] F. F. Kretschmer and B. L. Lewis, "Doppler properties of polyphase coded pulse compression waveforms," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-19, no. 4, pp. 521–531, Jul. 1983.
[30] F. F. Kretschmer, Jr., and K. Gerlach, "Low sidelobe radar waveforms derived from orthogonal matrices," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 27, no. 1, pp. 92–102, Jan. 1991.
[31] 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.
[32] T.-K. Lee and K. Yang, "The induced correlations of Zadoff–Chu sequences," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun./Jul. 2014, pp. 1648–1652.
[33] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming-correlation properties," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 90–94, Jan. 1974.
[34] N. Levanon and A. Freedman, "Ambiguity function of quadriphase coded radar pulse," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 25, no. 6, pp. 848–853, Nov. 1989.
[35] N. Levanon and E. Mozeson, *Radar signals*. New York, NY, USA: Wiley, 2004.
[36] B. L. Lewis and F. F. Kretschmer, "A new class of polyphase pulse compression codes and techniques," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-17, no. 3, pp. 364–372, May 1981.
[37] Y. Liu and P. Fan, "Modified Chu sequences with smaller alphabet size," *Electron. Lett.*, vol. 40, no. 10, pp. 598–599, May 2004.
[38] H. D. Luke, "Binary Alexis sequences with perfect correlation," *IEEE Trans. Commun.*, vol. 49, no. 6, pp. 966–968, Jun. 2001.
[39] S. L. Ma and W. S. Ng, "On non-existence of perfect and nearly perfect sequences," *Int. J. Inf. Coding Theory*, vol. 1, no. 1, pp. 15–38, 2009.
[40] 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.
[41] 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.
[42] W. H. Mow, "Unified perfect roots-of-unity sequences construction, and its use for designing better preambles than Zadoff–Chu sequences," in *Proc. 7th Int. Workshop Signal Design Appl. Commun. (IWSDA)*, Bengaluru, India, Sep. 2015.
[43] A. Ostafe and I. E. Shparlinski, "Pseudorandomness and dynamics of Fermat quotients," *SIAM J. Discrete Math.*, vol. 25, no. 1, pp. 50–71, 2011.
[44] K.-H. Park, H.-Y. Song, and D. S. Kim, "Families of perfect polyphase sequences from the array structure of Fermat-quotient sequences and Frank–Zadoff sequences," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, Jun. 2015, pp. 1537–1540.
[45] B. M. Popović, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1406–1409, Jul. 1992.
[46] 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.
[47] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York, NY, USA: McGraw-Hill, 2002.
[48] M. Soltanalian and P. Stoica, "On prime root-of-unity sequences with perfect periodic correlation," *IEEE Trans. Signal Process.*, vol. 62, no. 20, pp. 5458–5470, Oct. 2014.
[49] L. Song and J. Shen, Eds., *Evolved Cellular Network Planning and Optimization for UMTS and LTE*. Boca Raton, FL, USA: CRC Press, 2011.
[50] M. Su, "New optimum frequency hopping sequences derived from Fermat quotients," in *Proc. 6th Int. Workshop Signal Design Appl. Commun.*, Tokyo, Japan, Oct. 2013, pp. 166–169.
[51] 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.
[52] N. Zhang and S. W. Golomb, "Polyphase sequence with low autocorrelations," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 1085–1089, May 1993.

Ki-Hyeon Park (S'12) received the BS and the MS degree in Electrical and Electronic Engineering from the Yonsei University of Seoul, Korea, in 2007 and 2009, respectively. He is currently a Ph.D candidate working in Yonsei University under the supervision of Prof. Hong-Yeop Song. His area of research interest includes cryptography, coding theory, and combinatorial mathematics.

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 served as a general co-chair of IEEE ITW 2015 in Jeju, Korea. 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, KIISC and KMS.

Dae-San Kim (M'05) received his BS and MS degrees in mathematics from Seoul National University, Seoul, Korea, in 1978 and 1980, respectively, and the Ph.D. degree in mathematics from University of Minnesota, Minneapolis, MN, in 1989. He is a professor in the Department of Mathematics at Sogang University, Seoul, Korea. He has been there since 1997, following a position at Seoul Womens University. His research interests include number theory (exponential sums, modular forms, zeta functions, p-adic analysis, umbral calculus) and coding theory. He is a member of AMS (American Mathematical Society) and IEEE.

Solomon W. Golomb (M'57–F'82–LF'07) was born May 31, 1932, in Baltimore, MD. He received his B.A. in 1951 from Hopkins and his M.A. and Ph.D. degrees from Harvard in 1953 and 1957, all in mathematics. After a Fulbright year (1955.1956) in Norway, he joined the staff at the Jet Propulsion Laboratory (1956) as a Senior Research Engineer, becoming Group Leader of the Information Processing Group (1958), and Deputy Chief of the Telecommunications Research Section (1960). In 1963 he joined the faculty of the University of Southern California, where he holds the rank of Distinguished and University Professor, with a joint appointment in Electrical Engineering and Mathematics. At USC, he was President of the Faculty Senate (1976.1977), Vice Provost for Research (1986.1989), and Director of Technology.Annenberg Center for Communication (1995.1998). The central theme of his research has been developing and applying concepts of discrete mathematics to signal design for secure, reliable, and synchronized communications. He has published over 200 technical papers, and is author or coauthor of five books currently in print. He is a Fellow of the IEEE and of the AAAS. He has served on the Board of Governors of the Information Theory Society, and was its Shannon Lecturer in 1985. He was elected to the U.S. National Academy of Engineering (1976); to the U.S. National Academy of Sciences in 2003; and to the Russian Academy of Natural Sciences (1994) as a foreign member. His numerous awards include three honorary doctorate degrees; the Hamming Gold Medal of the IEEE; and the William Procter Prize of Sigma Xi. In 2013, he received the National Medal of Science from President Obama, and he will receive the Franklin Institute's 2016 Benjamin Franklin Medal in Electrical Engineering.