PAPER *Special Section on Signal Design and Its Applications in Communications*

Optimal Families of Perfect Polyphase Sequences from Cubic Polynomials*

Min Kyu SONG[†a)], ***Nonmember and*** **Hong-Yeop SONG**[†b)], ***Member***

SUMMARY For an odd prime p and a positive integer $k \geq 2$, we propose and analyze construction of perfect p^k-ary sequences of period p^k based on cubic polynomials over the integers modulo p^k. The constructed perfect polyphase sequences from cubic polynomials is a subclass of the perfect polyphase sequences from the Mow's unified construction. And then, we give a general approach for constructing optimal families of perfect polyphase sequences with some properties of perfect polyphase sequences and their optimal families. By using this, we construct new optimal families of p^k-ary perfect polyphase sequences of period p^k. The constructed optimal families of perfect polyphase sequences are of size $p-1$.

key words: *perfect polyphase sequences, cubic polynomials, optimal families of perfect polyphase sequences*

1. Introduction

Various sequences have been widely used in modern digital communication systems [8], [10], [11] and radar systems [14]. Recent applications include such commercial mobile communication systems as CDMA, WCDMA, and 3GPP LTE [1] and global navigation satellite systems as GPS [2] and GALILEO [7]. These applications require sequences with good correlation, or the minimum possible correlation magnitude for all the non-trivial phase shifts. Thus, it is best that sequences for these applications have zero autocorrelation at all out-of-phases, and such sequences are called perfect sequences.

A sequence is called a polyphase sequence if all the symbols are on the complex unit circle [8], [16], [18]. For many decades, perfect polyphase sequences (PPSs) have attracted engineers and researchers [5], [6], [9], [12], [15], [16], [18]–[20], [24]. For an integer $N \geq 2$, Frank and Zadoff constructed N-ary sequences of period N^2 in 1962 [9]. There is another class of PPSs, called the Zadoff-Chu sequence, whose phase sequence are generated by a quadratic polynomials. This class was proposed by Chu in 1972 [5], and generalized by Popovic [20]. A generalized version of Chu's sequences was named generalized chirp-like sequences by Popovic. In [16], [18], Mow classified all the known PPSs into four classes: the generalized Frank sequence [12, Theorem 3], the generalized chirp-like sequence [20], the Milewski sequence [15], and the PPS associated with some generalized bent functions [6].

In 1979, Sarwate showed that crosscorrelation magnitude of any two perfect sequences of the same length is greater than or equal to the square root of their length. After Sarwate's work, many constructions for PPS families, which achieve the Sarwate bound, have been proposed. These are based on the original Frank sequences [3], [17], [24] and the generalized Frank sequences [19], [23], the generalized chrip-like polyphase sequences [20]. Mow also considered optimal families of PPSs from his first unified construction [16] for some parameters.

Our work on generating PPSs from cubic polynomials and constructing their optimal families is motivated by the Zadoff-Chu sequence and the generalized chirp-like polyphase sequence which generated by using quadratic polynomials. In this paper, after reviewing some preliminaries in Sect. 2, we propose a construction of PPSs by using cubic polynomials over the integers modulo an odd prime power in Sect. 3. After then, in Sect. 4, we give some properties of PPSs and a general approach for constructing optimal families of PPSs. Based on the approach, we construct optimal families of PPSs from cubic polynomials. The constructed optimal families are new and of size $p-1$. We summarize our results with some concluding remarks in Sect. 5.

2. Preliminaries

2.1 Perfect Polyphase Sequences

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

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{n=0}^{N-1} a(n+\tau)b^*(n),$$

where $n+\tau$ is computed over the integers modulo N the asterisk symbol means the complex conjugate. If $\mathbf{b}$ is a cyclic shifted version of $\mathbf{a}$, then $C_{\mathbf{a},\mathbf{b}}(\tau)$ is called autocorrelation of $\mathbf{a}$ and denote by $C_{\mathbf{a}}(\tau)$, simply. Otherwise, it is called crosscorrelation.

A sequence $\mathbf{a} = \{a(n)\}_{n=0}^{N-1}$ is called perfect, if its autocorrelation magnitude is always zero for any $\tau \not\equiv 0 \pmod N$. There is a well-known lower-bound (so-called

Manuscript received January 8, 2018.
Manuscript revised July 24, 2018.

[†]The authors are with Yonsei University, Seoul, Korea.

*This work has been supported by the National GNSS Research Center Program of Defense Acquisition Program Administration and Agency for Defense Development. This paper was presented in part at 2017 International Symposium on Information Theory.

a) E-mail: mk.song@yonsei.ac.kr
b) E-mail: hysong@yonsei.ac.kr

DOI: 10.1587/transfun.E101.A.2359

the Sarwate bound) on the maximum crosscorrelation magnitude of perfect sequences [22]. The bound tell us that, for any two perfect sequences of period N, their maximum crosscorrealtion magnitude is always greater than or equal to square root of the length $\sqrt{N}$. We refer a pair of perfect sequences of period N to 'optimal pair' (with respect to the Sarwate bound) if their maximum crosscorrelation magnitude is $\sqrt{N}$. And, in the similar fashion, we refer a set of perfect sequences to 'optimal families of perfect sequences' (with respect to the Sarwate bound) if any pair of sequences in the set is an optimal pair.

A sequence $\mathbf{x}$ is called a polyphase sequence if all the terms of $\mathbf{x}$ is on the unit circle over the complex plane.

2.2 The Normalized DFT

For some purpose, we will use the normalized discrete Fourier transform (DFT). Let $\omega_N = e^{\frac{2\pi\sqrt{-1}}{N}}$ be a primitive N-th root of unity over the complex numbers, and $\mathbf{x} = \{x(n)\}_{n=0}^{N-1}$ be a sequence of length N over the complex field. Then, N-point normalized DFT of $\mathbf{x}$, denoted by $\mathbf{X} = \{X(l)\}_{l=0}^{N-1}$, is

$$X(l) = \mathfrak{F}\{x(n)\}(l) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n)\omega_N^{-ln}.$$

The inverse N-point normalized DFT of $\mathbf{X}$ is

$$x(n) = \mathfrak{F}^{-1}\{X(l)\}(n) = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} X(l)\omega_N^{ln}.$$

As shown in the above, throughout this paper, we will use small bold letters and capital bold letters with the same alphabet for representing 'time-domain' sequences and their 'frequency-domain' sequences, respectively.

Any pair of sequences $\mathbf{x} = \{x(n)\}_{n=0}^{N-1}$ and $\mathbf{X} = \{X(l)\}_{l=0}^{N-1}$ satisfies certain relation, which is usually referred as the Parseval's theorem. The following is the Parseval's theorem for the normalized DFT.

Lemma 1 (Parseval's theorem) *Let $\mathbf{x} = \{x(n)\}_{n=0}^{N-1}$ be a complex sequence of period N and $\mathbf{X} = \{X(l)\}_{l=0}^{N-1}$ be the frequency domain sequence of $\mathbf{x}$. Then,*

$$\sum_{n=0}^{N-1} |x(n)|^2 = \sum_{l=0}^{N-1} |X(l)|^2.$$

For the simplicity, here after, we use the term DFT instead of the normalized DFT.

3. PPSs from Cubic Polynomials

3.1 PPSs Constructed by Cubic Polynomials

In the remaining of this paper, we assume the following notation:

- p is an odd prime.
- $k \geq 2$ is a positive integer.
- ω_N is a complex primitive N-th root of unity.
- $\mathbb{Z}$ is the set of integers and $\mathbb{Z}_{p^k}$ is the set of integers modulo p^k.

Let a cubic polynomial $f(n)$ for $n \in \mathbb{Z}_{p^k}$ be given as follows:

$$f(n) = an^3 + bn^2 + cn + d \pmod{p^k}, \tag{1}$$

where a, b, c, and d are integers in $\mathbb{Z}_{p^k}$. We can construct a p^k-ary sequence $\mathbf{f} = \left\{\omega_{p^k}^{f(n)}\right\}_{n=0}^{p^k-1}$ of length p^k as an evaluation of $f(n)$ over $\mathbb{Z}_{p^k}$. It may be obvious that the choice of d does not affect the autocorrelation magnitude of $\mathbf{f}$, since it contributes to the sequence only as a constant phase shift of all the terms in one period. Thus, we will mainly focus on the choice of a, b, and c, and we simply assume that $d = 0$ in the remaining without loss of generality.

The Zadoff-Chu sequence is a well-known class of PPSs whose phase sequences is generated by quadratic polynomials [5]. They are defined to have any period N, but we are interested in the case where $N = p^k$ for an odd prime p and a positive integer k. In this case, a p^k-ary Zadoff-Chu sequence of period p^k is defined by

$$\mathbf{z} = \left\{\omega_{p^k}^{z(n)}\right\} = \left\{\omega_{p^k}^{gn(n+1)/2+hn \pmod{p^k}}\right\}_{n=0}^{p^k-1}, \tag{2}$$

where $g \not\equiv 0 \pmod{p}$ and h is an integer.

Proposition 1 *If $a \equiv 0 \pmod{p^k}$, $b \not\equiv 0 \pmod{p}$, then the sequence $\mathbf{f}$ constructed above by $f(n)$ in (1) becomes a p^k-ary Zadoff-Chu sequence of period p^k with parameters $g = 2b$ and $h = c - 2b$, where g, h are defined in (2).*

Proof *Observe that*

$$\begin{aligned} f(n) &= bn^2 + cn \\ &= 2bn(n+1)/2 + (c-2b)n. \end{aligned}$$

By letting $g = 2b$ and $h = c - 2b$, we get the conclusion. ■

Remark 1 *A Zadoff-Chu sequence is constructed using a quadratic polynomial.*

Now, we show that there are other choices of a, b, c, which also generate PPSs, especially, when $a \not\equiv 0 \pmod{p^k}$. For our purpose, a quadratic exponential sum in [16, Lemma 3.1] is useful. For any positive integer q, and any $u, v \in \mathbb{Z}$, we have

$$\left|\sum_{n=0}^{q-1} \omega_q^{un^2+vn}\right| = \begin{cases} \delta q, & \text{if } \gamma \text{ is odd and } v \equiv 0 \pmod{\delta} \\ 2\delta q, & \text{if } \gamma \text{ is even and } v \equiv \delta\alpha(\gamma/2) \pmod{2\delta} \\ 0, & \text{else,} \end{cases}$$

where $\delta = \gcd(u, q)$, $\alpha = u/\delta$, and $\gamma = q/\delta$.

Here we note that, when q is odd, γ must be odd also. So, if $q = p^k$ is an odd prime power, then the quadratic exponential sum becomes following:

Lemma 2 (Modified version of [16, Lemma 3.1]) *For any integers u and v, we have*

$$\left|\sum_{n=0}^{p^k-1} \omega_{p^k}^{un^2+vn}\right|^2 = \begin{cases} \delta p^k, & \text{if } v \equiv 0 \pmod{\delta} \\ 0, & \text{otherwise.} \end{cases}$$

where $\delta = \gcd(u, p^k)$.

Theorem 1 *Consider the sequence* $\mathbf{f}$ *constructed above by the polynomial $f(n)$ in* (1).

1. *Let $p = 3$. If $a \not\equiv 0 \pmod{p^k}$, $b \not\equiv 0 \pmod{p}$, then the sequence* $\mathbf{f}$ *is perfect and of period p^k for any c.*
2. *Let $p \geq 5$. If $a \not\equiv 0 \pmod{p^k}$, $b \not\equiv 0 \pmod{p}$, and $a \equiv 0 \pmod{p}$, then the sequence* $\mathbf{f}$ *is perfect and of period p^k for any c.*

Proof *For any τ, the autocorrelation of the sequence* $\mathbf{f}$ *is given by*

$$\begin{aligned} \mathrm{C}_{\mathbf{f}}(\tau) &= \sum_{n=0}^{p^k-1} \omega_{p^k}^{f(n+\tau)-f(n)} \\ &= \sum_{n=0}^{p^k-1} \omega_{p^k}^{3a\tau n^2+(3a\tau^2+2b\tau)n+\epsilon} \qquad (3) \\ &= \omega_{p^k}^{\epsilon} \sum_{n=0}^{p^k-1} \omega_{p^k}^{3a\tau n^2+(3a\tau^2+2b\tau)n}, \qquad (4) \end{aligned}$$

where $\epsilon = a\tau^3 + b\tau^2 + c\tau$. Let $u = 3a\tau$, $v = 3a\tau^2 + 2b\tau$. Assume that $\tau \not\equiv 0 \pmod{p^k}$. Now, we will check that $v \not\equiv 0 \pmod{\delta}$ where $\delta = \gcd(u, p^k)$. If this holds, then by Lemma 2, we conclude that $C_{\boldsymbol{f}}(\tau) = 0$ for any $\tau \not\equiv 0 \pmod{p^k}$.

1. *Let $p = 3$, $a \not\equiv 0 \pmod{3^k}$, $b \not\equiv 0 \pmod{p}$, and $\tau \not\equiv 0 \pmod{p^k}$, and $\delta = \gcd(u, 3^k) = \gcd(3a\tau, 3^k)$. Since $\delta | 3a\tau$,*

   $$v \equiv 2b\tau \pmod{\delta}.$$

   Now we claim that $v \not\equiv 0 \pmod{\delta}$. To prove the claim, we write

   $$\tau = t3^r$$

   for some t and r with $\gcd(t, 3) = 1$ and $0 \leq r \leq k-1$. Suppose on the contrary that

   $$v \equiv 2b\tau \equiv 2bt3^r \equiv 0 \pmod{\delta}. \qquad (5)$$

   Observe that

   $$\delta = \gcd(3a\tau, 3^k) = \gcd(ta3^{r+1}, 3^k).$$

   Therefore, (5) *implies that*

   $$\gcd(ta3^{r+1}, 3^k l) | 3^r$$

   or

   $$3^{r+1} \gcd(at, 3^{k-(r+1)}) | 3^r,$$

   which is a contradiction since $\gcd(at, 3^{k-(r+1)}) \geq 1$.
2. *It can be similarly done.* ∎

We would like to note that, when $a \not\equiv 0 \pmod{p^k}$, $b \equiv 0 \pmod{p}$, there exists some τ which makes $v = 3a\tau^2 + 2b\tau \equiv 0 \pmod{\delta}$, where $\delta = \gcd(3a\tau, p^k)$. In that case, by Lemma 2, the magnitude of the out-of-phase autocorrelation of the sequence $\mathbf{f}$ at the phase shift τ becomes $\sqrt{\delta p^k} > 0$.

In the remaining of this paper, we assume that a, b, and c are chosen according to Theorem 1 to force $\mathbf{f}$ be a PPS.

3.2 Relationship with Previous PPSs

Before 1993, it was known that previous PPSs can be divided into four classes. When we restrict their length to power of p, then, they are of the following forms. Here, we let $p^k = p^{2u+v}$ with $0 \leq v \leq 1$, $n = qp^u + r$ with $0 \leq r < p^u$, and $m(r)$ be an arbitrary function over $\mathbb{Z}_{p^k}$.

1. **(P1) the generalized Frank sequence [12, Theorem 3]**
   This class exists only for $v = 0$ and the generalized Frank sequence $\mathbf{s}_1 = \left\{\omega_{p^k}^{s_1(n)}\right\}_{n=0}^{p^k-1}$ is given by

   $$s_1(n) = s_1(qp^u + r) = qp^u\pi(r) + m(r).$$

   Here, $\pi(r)$ is a permutation over $\mathbb{Z}_{p^u}$.

2. **(P2) the generalized chirp-like polyphase sequence [20]**
   For any k, the generalized chirp-like sequence $\mathbf{s}_2 = \left\{\omega_{p^k}^{s_2(n)}\right\}_{n=0}^{p^k-1}$ is given by

   $$\begin{aligned} s_2(n) &= s_2(qp^u + r) \\ &= \mu p^{2u} q^2 + (2\mu p^u r + \lambda p^u)q + m(r), \end{aligned}$$

   where μ, λ are integers with $\gcd(\mu, p) = 1$. This class of PPSs includes the Zadoff-Chu sequences.

3. **(P3) the Milewski sequence [15]**
   This class exists only for $v = 1$ and the Milewski sequence $\mathbf{s}_3 = \left\{\omega_{p^k}^{s_3(n)}\right\}_{n=0}^{p^k-1}$ is given by

   $$\begin{aligned} s_3(n) &= s_3(qp^u + r) \\ &= p^{2u}(\zeta q^2 + \eta q) + p^u\theta qr + \kappa \\ &= \zeta p^{2u} q^2 + (\eta p^{2u} + \theta p^u r)q + \kappa, \end{aligned}$$

   where ζ, θ are coprime to p and η, κ are any integers.

4. **(P4) the PPSs from generalized bent functions due to Chung and Kumar [13]**

   The PPS $\mathbf{s}_4 = \left\{\omega_{p^k}^{s_4(n)}\right\}_{n=0}^{p^k-1}$ is given by

$$\begin{aligned} s_4(n) &= s_4(qp^u + r) \\ &= ep^{2u}q^2 + (2ep^u r + \xi p^u - ep^{2u})q + m(r) \end{aligned}$$

   where e is an integer coprime to p and ξ is any integer in $\mathbb{Z}_{p^{u+v}}$.

In 1993, Mow proposed a unified construction of PPSs. The unified construction was further improved in 1996 as following:

5. **the Mow's unified construction [18]**

   A PPS over $\mathbf{s_u} = \left\{\omega_{p^k}^{s_u(n)}\right\}_{n=0}^{p^k-1}$ can be constructed by using

$$\begin{aligned} s_u(n) &= s_u(qp^u + r) \\ &= p^{2u}\alpha(r)q^2 + p^u\beta(r)q + m(r), \end{aligned}$$

   where $\alpha(r)$ is a function with $(\alpha(r), p) = 1$ for any $r \in \mathbb{Z}_{p^u}$, $\beta(r)$ is a function such that $\beta(r) \pmod{p^u}$ is a permutation over $\mathbb{Z}_{p^u}$.

Mow showed that the unified construction include all the PPSs constructions of P1-P4.

Recall that phase the n-th term of the PPS $\mathbf{f}$ is given by (1) where

- If $p = 3$, then $a \not\equiv 0 \pmod{p^k}$, $b \not\equiv 0 \pmod{p}$
- If $p \geq 5$, then $a \not\equiv 0 \pmod{p^k}$, $b \not\equiv 0 \pmod{p}$, and $a \not\equiv 0 \pmod{p}$.

Let $p^k = p^{2u+v}$. Then, $f(n)$ in (1) becomes following:

$$\begin{aligned} &f(qp^u + r) \\ &= a\left(qp^u + r\right)^3 + b\left(qp^u + r\right)^2 + c\left(qp^u + r\right) \\ &= a\left(q^3p^{3u} + 3q^2p^{2u}r + 3qp^u r^2 + r^3\right) \\ &\quad + b\left(q^2p^{2u} + 2qrp^u + r^2\right) + c\left(qp^u + r\right) \\ &= ap^{3u}q^3 + p^{2u}\left(3ar + b\right)q^2 + p^u\left(3ar^2 + 2br + c\right)q \\ &\quad + ar^3 + br^2 + cr. \end{aligned}$$

Note that $p^{3u} \equiv 0 \pmod{p^k}$. And, if we let $\chi(r) = ar^3 + br^2 + cr$ for the simplicity, then, finally, we get

$$\begin{aligned} &f(qp^u + r) \\ &= p^{2u}\left(3ar + b\right)q^2 + p^u\left(3ar^2 + 2br + c\right)q + \chi(r). \end{aligned} \tag{6}$$

Lemma 3 (Quadratic permutation polynomial [21]) *Let p be an odd prime and k be a positive integer with $k \geq 2$. Then, a quadratic polynomial*

$$ax^2 + bx + c$$

is a permutation polynomial over the integers modulo p^k if and only if $a \equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$.

Theorem 2 *Let $\mathbf{f} = \left\{\omega_{p^k}^{f(n)}\right\}_{n=0}^{p^k-1}$ be a PPS from a cubic polynomial and $p^k = p^{2u+v}$ with $0 \leq v \leq 1$.*

1. *If $v = 0$, then $\mathbf{f}$ is a generalized Frank sequence.*
2. *If $v = 1$ and $p^u \mid 3a$, then $\mathbf{f}$ is a generalized chirp-like polyphase sequence.*
3. *If $v = 1$ and $p^u \nmid 3a$, then $\mathbf{f}$ is not in any class of P1-P4. But, it can be constructed by using the Mow's unified construction.*

Proof 1. *Observe that, if $v = 0$, (6) becomes*

$$p^u\left(3ar^2 + 2br + c\right)q + \chi(r).$$

And, by Lemma 3, $3ar^2 + 2br + c$ is a quadratic permutation polynomial over $\mathbb{Z}_{p^u}$ for any a, b, and c chosen by Theorem 1.

2. *Observe that, if $v = 1$ and $p^u \mid 3a$, (6) becomes*

$$bp^{2u}q^2 + \left(2bp^u r + cp^u\right)q + \chi(r).$$

3. *It is enough to see that $\gcd(3ar + b, p) = 1$ for any r and $3ar^2 + 2br + c$ is a quadratic permutation polynomial over $\mathbb{Z}_{p^u}$.* ■

Therefore, the PPS construction by using cubic polynomials is not a new one. But, to the best of our knowledge, there is no result on constructing optimal families of PPSs each of which has a phase sequence evaluated by cubic polynomials.

Since the PPSs from cubic polynomials is a subclass of the PPSs generated by Mow's unified construction, they have the following property. PPSs which have that property is known to be 'modulatable sequences.'

Corollary 1 *Let $\mathbf{f} = \left\{\omega_{p^k}^{f(n)}\right\}_{n=0}^{p^k-1}$ be a PPS from a cubic polynomial. And, let $p^k = p^{2u+v}$ with $0 \leq v \leq 1$ and write $n = qp^u + r$. Then, for any function $m(r)$ over the integers modulo $\mathbb{Z}_{p^k}$,*

$$\mathbf{f}' = \left\{\omega_{p^k}^{f(n)+m(r)}\right\}$$

is a PPS of period p^k.

4. Optimal PPS Family Construction

Before we construct optimal families of PPSs from cubic polynomials, we will discuss some interesting properties of PPSs and their optimal families.

Lemma 4 *Let $\mathbf{s} = \{s(n)\}_{n=0}^{N-1}$ be a polyphase sequence of period N. Then, $\mathbf{s}$ is a PPS if and only if its DFT, denoted by $\mathbf{S} = \{S(k)\}_{k=0}^{N-1}$, is also a PPS.*

Proof *(⇒) Assume that* $\mathbf{s}$ *is a PPS. We first show that* $\mathbf{S}$ *is a polyphase sequence. By the assumption,*

$$\begin{aligned} C_s(\tau) &= \sum_{n=0}^{N-1} s(n)s^*(n+\tau) \\ &= N\delta(\tau). \end{aligned}$$

where

$$\delta(\tau) = \begin{cases} 1, & \tau = 0 \\ 0, & \text{otherwise.} \end{cases}$$

is the Kronecker delta. Obviously,

$$\mathfrak{F}\{C_s(\tau)\}(l) = N\mathfrak{F}\{\delta(n)\} = \sqrt{N}.$$

Observe that

$$\begin{aligned} \mathfrak{F}\{C_s(\tau)\}(l) &= \frac{1}{\sqrt{N}} \sum_{\tau=0}^{N-1} C_s(\tau)\omega^{-l\tau} \\ &= \frac{1}{\sqrt{N}} \sum_{\tau=0}^{N-1} \sum_{n=0}^{N-1} s(n)s^*(n+\tau)\omega^{-l\tau} \\ &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} s(n)\omega^{ln} \sum_{\tau=0}^{N-1} s^*(n+\tau)\omega^{-l(n+\tau)} \\ &= \sqrt{N}S(-l)S^*(-l) \\ &= \sqrt{N}\,|S(-l)|^2\,. \end{aligned}$$

Therefore, $|S(l)| = 1$ *for any* $l = 0, 1, ..., N-1$. *In other words,* $\mathbf{S}$ *is a polyphase sequence.*

The remaining is showing that $\mathbf{S}$ *is perfect. Observe that*

$$\begin{aligned} &C_{\mathbf{S}}(\mu) \\ &= \sum_{l=0}^{N-1} S(l)S^*(l+\mu) \\ &= \sum_{l=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} s(n)\omega^{-ln} \right) S^*(l+\mu) \\ &= \sum_{n=0}^{N-1} s(n) \left(\frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} S(l+\mu)\omega^{(l+\mu)n} \right)^* \omega^{\mu n} \\ &= \sum_{n=0}^{N-1} |s(n)|^2 \omega^{\mu n} \end{aligned}$$

Since $\mathbf{s}$ *is polyphase,* $|s(n)|^2 = 1$ *for any* $n = 0, 1, ..., N-1$. *Therefore, we conclude that*

$$C_{\mathbf{S}}(\mu) = \sum_{n=0}^{N-1} \omega^{\mu n} = N\delta(\mu).$$

(⇐) We omit the proof because it can be proved by the similar process. ∎

Assume that $\mathbf{a} = \{a(n)\}_{n=0}^{N-1}$ and $\mathbf{b} = \{b(n)\}_{n=0}^{N-1}$ form an optimal pair of PPSs. Then, by Lemma 4, $|A(l)B^*(l)| = 1$ for any $l = 0, 1, ..., N-1$. Now, observe that

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{n=0}^{N-1} a(n)b^*(n+\tau) \\ &= \sum_{n=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} A(l)\omega_N^{ln} b^*(n+\tau) \\ &= \sum_{l=0}^{N-1} A(l) \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} b^*(n+\tau)\omega_N^{ln} \\ &= \sum_{l=0}^{N-1} A(l)B^*(l)\omega_N^{-l\tau}. \end{aligned}$$

The last expression yields that $\left\{ \frac{1}{\sqrt{N}} C_{a,b}(\tau) \right\}_{\tau=0}^{N-1}$ and $\{A(l)B^*(l)\}_{l=0}^{N-1}$ form a DFT pair. This lead us to the following theorem:

Theorem 3 *Let* $\mathbf{a} = \{a(n)\}_{n=0}^{N-1}$ *and* $\mathbf{b} = \{b(n)\}_{n=0}^{N-1}$ *be two PPSs of period* N. *Then,* $\mathbf{a}$ *and* $\mathbf{b}$ *form an optimal pair of PPSs if and only if the crosscorrelation magnitude of* $\mathbf{a}$ *and* $\mathbf{b}$ *is* $\sqrt{N}$ *for any shift.*

Proof *(⇒) We start the proof from the fact that* $\frac{1}{\sqrt{N}} C_{a,b}(\tau)$ *and* $A(l)B^*(l)$ *form a DFT pair. By using Lemma 1, we have*

$$\sum_{\tau=0}^{N-1} |C_{\mathbf{a},\mathbf{b}}(\tau)|^2 = N \sum_{k=0}^{N-1} |A(l)B^*(l)|^2 = N^2. \tag{7}$$

Now, suppose on the contrary that $|C_{\mathbf{a},\mathbf{b}}(\tau)| < \sqrt{N}$ *for some* τ. *Then, since* $\mathbf{a}$ *and* $\mathbf{b}$ *should satisfy* (7), *there must be some* τ' *such that* $|C_{\mathbf{a},\mathbf{b}}(\tau')| > \sqrt{N}$. *This is a contradiction. Therefore,* $|C_{\mathbf{a},\mathbf{b}}(\tau)| = \sqrt{N}$ *for any* τ.

(⇐) It is straightforward by the definition of optimal pair of perfect sequences. ∎

Corollary 2 *Let* $\mathcal{F}$ *be a set of PPSs. Then,* $\mathcal{F}$ *is an optimal family if and only if* $C_{\mathbf{a},\mathbf{b}}(\tau) = \sqrt{N}$ *for any two distinct sequences* $\mathbf{a}, \mathbf{b} \in \mathcal{F}$ *and any shift* τ.

Now, we will give a general construction for optimal PPS families. This construction is based on the following lemma:

Lemma 5 ([4]) *Let* $\mathbf{a} = \{a(n)\}_{n=0}^{N-1}$ *be a perfect sequence with* $C_{\mathbf{a}}(0) = N$. *Then,*

$$\left| \sum_{n=0}^{N-1} a(n) \right| = \sqrt{N}.$$

Theorem 4 (Optimal family construction) *Let* $\mathcal{F}$ *be a set of PPSs. If* $\{a(n)b^*(n+\tau)\}_{n=0}^{N-1}$ *is a PPS for any* $\mathbf{a}, \mathbf{b} \in \mathcal{F}$ *and any* τ, *then* $\mathcal{F}$ *is optimal.*

Based on this, we can easily construct optimal PPS

families from cubic polynomials as follows:

Corollary 3 *For a prime power $p^k = p^{2v+u}$ with $0 \le v \le 1$, let $\mathcal{S} = \{\mathbf{f}_1, \mathbf{f}_2, ...\mathbf{f}_M\}$ be a set of PPSs of period p^k from cubic polynomials in which the i-th sequence is given by*

$$\mathbf{f}_i = \left\{\omega_{p^k}^{f_i(n)}\right\}_{n=0}^{p^k-1} = \left\{\omega_{p^k}^{a_i n^3 + b_i n^2 + c_i n + m_i(r)}\right\}_{n=0}^{p^k-1},$$

where $n = qp^u + r$ with $0 \le r < p^u$ and $m_i(r)$ is an arbitrary function over $\mathbb{Z}_{p^k}$. If the coefficients $b_1, b_2, ..., b_M$ satisfy

$$b_i - b_j \not\equiv 0 \pmod{p}$$

for any $1 \le i < j \le M$, then $\mathcal{S}$ is an optimal family.

Proof *We first show the case where $m_i(r) = 0$ for any i and r. For any i, j with $i \ne j$, we have*

$$\begin{aligned} & f_i(n+\tau) - f_j(n) \\ &= a_i n^3 + b_i n^2 + c_i n - (a_j n^3 + b_j n^2 + c_j n) \\ &\quad + 3a_i \tau n^2 + (3a_i \tau^2 + 2b_i \tau) n + \epsilon \\ &= (a_i - a_j) n^3 + (b_i + 3a_i \tau - b_j) n^2 \\ &\quad + (c_i - c_j + 3a_i \tau + 2b_i \tau) n + \epsilon, \end{aligned} \tag{8}$$

where $\epsilon = a\tau^3 + b\tau^2 + c\tau$. Now, assume that

$$b_i - b_j \not\equiv 0 \pmod{p},$$

for any $i \ne j$. If $a_i \equiv a_j \pmod{p^k}$, then, the RHS of (8) is phase sequence of a Zadoff-Chu of period p^k. (This can be shown by similar process of the proof of Proposition 1.) And, if $a_i \not\equiv a_j \pmod{p^k}$, then, by Theorem 1,

$$\left\{\omega_{p^k}^{f_i(n+\tau) - f_j(n)}\right\}_{n=0}^{p^k-1} \tag{9}$$

is a PPS for any τ. Therefore, by Theorem 4, $\mathcal{S}$ is an optimal family of PPSs. For the case where $m_i(r)$ is an arbitary function, by using Corollary 1, it can be easily shown that the sequence in (9) is perfect, and hence, $\mathcal{S}$ is an optimal family. ■

Corollary 4 *In any optimal family $\mathcal{S}$ constructed by using Corollary 3, there are at most $p-1$ sequences.*

Proof *Note that there are exactly $p-1$ integers which are not congruent to each other over the integers modulo p. Therefore, the number of sequences in $\mathcal{S}$ is at most $p-1$.* ■

The size $p-1$ can be simply achieved by just letting all the b_i's be not congruent to each other over the integers modulo p.

Corollary 5 *Let $\mathcal{S}$ be an optimal family constructed by using Corollary 3. Even though we replace a sequence*

$$\left\{\omega_{p^k}^{an^3 + bn^2 + cn + m(r)}\right\}_{n=0}^{p^k-1}$$

in $\mathcal{S}$ with a generalized chirp-like polyphase sequence given by

$$\left\{\omega_{p^k}^{bn^2 + cn + m(r)}\right\}_{n=0}^{p^k-1},$$

the result is also an optimal PPS family.

Remark 2 *Note that, for the proposed optimal PPS families of period p^k, the size is always $p-1$ even if the period p^k of each sequence becomes longer. One interesting point is that, for the period p^k, the optimal families constructed in [16], [17], [19], [20], [23], [24] are also of size $p-1$. Until now, it is unclear whether $p-1$ is the maximum achievable size or not.*

5. Concluding Remarks

Throughout this paper, we discuss a construction for p^k-ary PPSs of period p^k whose phase sequence is evaluated by cubic polynomials, and we compare it with the previous known PPSs constructions. And then, after describing some general properties PPSs and their optimal pairs (or optimal families), we give a general approach for constructing optimal PPS families. Here, we would like to note that the general approach in Theorem 4 can be applied for any other PPSs to construct optimal families without complex calculation for showing their optimality. By using the general approach, we obtain new optimal families of p-ary PPSs of period p^k each of which comes from cubic polynomials. The constructed optimal families are of size $p-1$. As mentioned in Remark 2, all the known optimal PPS families of period p^k has of size $p-1$. It would be an interesting problem to answer to the question: what is the limit on the size of optimal PPS families of period an odd prime power p^k?

References

[1] Physical Channels and Modulation (Release 13), 3GPP TS 36.211 V13.4.0, Jan. 2017.
[2] Global positioning systems directorate systems engineering & integration interface specification, IS-GPS-200H, March 2014.
[3] W. Alltop, "Decimations of the Frank-Heimiller sequences," IEEE Trans. Inf. Theory, vol.32, no.7, pp.851–853, July 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.18, no.4, pp.531–532, July 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] H. Ebner, Galileo overall architecture definition: SIS frequency characteristics, GALA-ASTR-DD-019, issue 5.0, Nov. 2000.
[8] P. Fan and M. Darnell, Sequence Design for Communications Applications, John Wiley & Sons, Exter, 1996.
[9] R. Frank and S. Zadoff, "Phase shift pulse codes with good periodic correlation properties (corresp.)," IRE Trans. Inf. Theory, vol.8, no.6, pp.381–382, Oct. 1962.
[10] S.W. Golomb and G. Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar, Cambridge

University Press, New York, 2005.
[11] J.-H. Kim and H.-Y. Song, "Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," J. Commun. Netw., vol.1, no.1, pp.14–18, March 1999.
[12] P.V. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized bent functions and their properties," J. Combinat. Theory A, Series A, vol.40, no.1, pp.90–107, Sept. 1985.
[13] H. Chung and P.V. Kumar, "A new general construction for generalized bent function," IEEE Trans. Inf. Theory, vol.35, no.1, pp.206–209, 1989.
[14] N. Levanon and E. Mozeson, Radar Signals, John Wiley & Sons, Hoboken, New Jersey, 2004.
[15] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," IBM J. Res. Dev., vol.27, no.5, pp.426–431, Sept. 1983.
[16] W.H. Mow, A study of correlation of sequences, Ph.D. dissertation, Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong, May 1993.
[17] W.H. Mow, "On the decimations of Frank sequences," IEEE Trans. Commun., vol.43, no.2/3/4, pp.751–753, Feb. 1995.
[18] W.H. Mow, "A new unified construction of perfect root-of-unity sequences," Proc. IEEE 4th International Symposium on Spread Spectrum Techniques and Applications, vol.3, pp.955–959, Sept. 1996.
[19] 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-qutient sequences," IEEE Trans. Inf. Theory, vol.62, no.2, pp.1076–1086, Feb. 2016.
[20] B.M. Popovic, "Generalized chirp-like polyphase sequences with optimum correlation properties," IEEE Trans. Inf. Theory, vol.38, no.4, pp.1406–1409, July 1992.
[21] J. Ryu and O.Y. Takeshita, "On quadratic inverses for quadratic permutation polynomials over integer rings," IEEE Trans. Inf. Theory, vol.52, no.3, pp.1254–1260, March 2006.
[22] D.V. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences (Corresp.)," IEEE Trans. Inf. Theory, vol.25, no.6, pp.720–724, Nov. 1979.
[23] M.K. Song and H.-Y. Song, "A construction of odd length generators for optimal families of perfect sequences," IEEE Trans. Inf. Theory, vol.64, no.4, pp.2901–2909, April 2018.
[24] 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.

Min Kyu Song received his B.S. degree in Electronic Engineering from Konkuk University, Seoul, Korea, and M.S. 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 Channel Coding and Crypto Lab. at Yonsei University. His area of research interest includes PN sequences, cryptography, and coding theory.

Hong-Yeop Song received his B.S. 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.