Technical Report 2020-001

Perfect polyphase sequences of the odd prime length

Takao Maeda, Yodai Watanabe, Takafumi Hayashi

May 11, 2020

Division of Computer Science
The University of Aizu
Tsuruga, Ikki-Machi, Aizu-Wakamatsu City
Fukushima, 965-8580 Japan

Technical Report 2020-001

Title:

Perfect polyphase sequences of the odd prime length

Authors:

Takao Maeda, Yodai Watanabe, Takafumi Hayashi

Key Words and Phrases:

perfect sequence, polyphase, root of unity, residue ring, parameterization,

Abstract:

Perfect polyphase sequences are famous for its variety of applications. We are interested in mathematical aspects of such sequences. Since they are defined intrinsically, it is important to reveal the structure of the set of such sequences. This paper fully characterizes perfect p-phase sequences of length p for an odd prime p. The characterization is given as the equivalence between the following two conditions (1) and (2) for a p-phase sequence $\{a_n\}_{n=0}^{p-1}$ with $a_n = {\omega_p}^{f_n}$ for $0 \leq n \leq p-1$, where ω_p denotes a primitive p-th root of unity:

(1)$\{a_n\}$ is perfect,

(2)f_n is a quadratic polynomial in n.

The complete proof is described. To analyze the structure of the set of such sequences, some easy transformations of the set are defined. For an arbitrary such sequence $\{a_n\}_{n=0}^{p-1}$, it is shown that there exists transformation χ such that χ is a composition of the easy transformations and $\chi(\{a_n\}_{n=0}^{p-1}) = \{\omega^{n^2}\}_{n=0}^{p-1}$.

Report Date:

5/11/2020

Written Language:

English

Any Other Identifying Information of this Report:

Distribution Statement:

First Issue: 12 copies

Supplementary Notes:

Mathematics and Physics Laboratory Group
The University of Aizu
Aizu-Wakamatsu
Fukushima 965-8580
Japan

Perfect polyphase sequences of the the odd prime length

TakaoMaeda Yodai Watanabe Takafumi Hayashi

May 11, 2020

Abstract

Perfect polyphase sequences are famous for its variety of applications. We are interested in mathematical aspects of such sequences. Since they are defined intrinsically, it is important to reveal the structure of the set of such sequences.

This paper fully characterizes perfect p-phase sequences of length p for an odd prime p. The characterization is given as the equivalence between the following two conditions (1) and (2) for a p-phase sequence $\{a_n\}_{n=0}^{p-1}$ with $a_n = {\omega_p}^{f_n}$ for $0 \leq n \leq p-1$, where ω_p denotes a primitive p-th root of unity:

(1) $\{a_n\}$ is perfect,

(2) f_n is a quadratic polynomial in n.

The complete proof is described.

To analyze the structure of the set of such sequences, some easy transformations of the set are defined. For an arbitrary such sequence $\{a_n\}_{n=0}^{p-1}$, it is shown that there exists transformation χ such that χ is a composition of the easy transformations and $\chi(\{a_n\}_{n=0}^{p-1}) = \{\omega^{n^2}\}_{n=0}^{p-1}$.

keywords: perfect sequence, polyphase sequence, p-phase sequence, root of unity, residue ring, parameterization

1 Introduction

A perfect polyphase sequence is known as perfect root-of-unity sequence (PRUS), perfect N-array sequence, perfect N-phase sequence. It is one of the important research theme of sequence design and is introduced in [1], which is published as a comprehensive text book of sequence design. Frank sequences, Chu sequences and another sequences are introduced in it as a perfect polyphase sequence. So the history of the research of perfect polyphase sequences can be trace back to the days of Frank[2] or Chu[3]. Much research has been done since then. A lot of methods to build it are proposed[6], and many properties have been revealed[7, 4] There are still a lot of application of perfect polyphase sequences. Many recent papers in this field seems to begin with samples of their applications. For example, synchronization, communication schemes (DS/SSMA, FH/SSMA) navigation (GPS, GALILEO), pulse-compression RADAR, active-SONAR, etc. are listed out in [4, 5]

We are interested in the mathematical aspects of perfect polyphase sequences. Perfect sequences or polyphase sequences are defined intrinsically, i.e. these sequences are defined as sequences which satisfy several equalities. It seems to be difficult to treat them.

We think that parameterization of such sequences are promising, to avoid such kind of difficulties. We tried to parameterize several types of sequences. We tried to parameterize a perfect sequence. Expanding the theory of discrete Fourier analysis, we succeeded to parameterize the set of perfect sequences of a general case[9, 10]. We could not parameterize the set of perfect polyphase sequences by using a similar method. We succeeded in parameterizing it with a completely different approach in the case of an odd prime length.

According to the result, arbitrary perfect polyphase sequence of odd prime length are expressed by the exponential function and a quadratic form. Preparing terminologies, symbols and definitions , we describe the result.

1.1 Terminologies

$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$, are the ring of integers, the field of rational numbers, the field of real numbers and the field of complex numbers, respectively. i is an imaginary unit, i.e. $i = \sqrt{-1} \in \mathbf{C}$. Let $z = x + iy \in \mathbf{C}$ be a complex number where $x, y \in \mathbf{R}$. The complex conjugate of z is expressed as z^*, i.e. $z^* = x - iy$.

Let A be a set. id_A is the identity mapping of A. $|A|$ is the number of elements belonging to A. Let R be a ring and X be an indeterminate. $R[X]$ is the polynomial ring of X over R.

Let N, m, n be integers such that $N > 1$. $\omega_N = e^{\frac{2\pi i}{N}}$ is a N-th root of unity. In the case N is obvious, N is abbreviated and we simply write ω. $\mathbf{Z}/N\mathbf{Z}$ is a quotient ring of $\mathbf{Z}$ by the ideal $N\mathbf{Z}$. $\overline{n}$ is an image of n by the canonical projection map $\mathbf{Z} \to \mathbf{Z}/N\mathbf{Z}$. $[m, n]$ is the greatest common divisor of m and n. If m is positive, we define the factorial of m as $m! = m \cdot (m-1) \cdots 2 \cdot 1$. If $m \geq n \geq 0$, the binomial coefficient ${}_mC_n$ is defined as follows;

$${}_mC_n = \frac{m!}{(m-n)!n!}$$

In the case of the calculation in $\mathbf{Z}/N\mathbf{Z}$, it should be treated as a quotient of integers and should not be treated as a quotient of elements of $\mathbf{Z}/N\mathbf{Z}$, since there is a possibility that $(m-n)!n! \equiv 0 \mod N$. $\mathbf{Z}_N$ and $\mathbf{Z}_N^\times$ are subsets of $\mathbf{Z}$ defined as follows;

$$\begin{aligned} \mathbf{Z}_N &= \{m \in \mathbf{Z} | 0 \leq m \leq N-1\} = \{0, 1, 2, \cdots, N-1\}, \\ \mathbf{Z}_N^\times &= \{m \in \mathbf{Z}_N | [m, N] = 1\}. \end{aligned}$$

1.2 Definitions and the main theorem

Definition. A sequence of length N is an array of complex numbers indexed by $\mathbf{Z}_N$ and is denoted as follows;

$$\{a_0, a_1, \cdots, a_{N-1}\},\ \ \{a_n\}_{n=0}^{N-1},\ \ \{a_n\}_{0\leq n\leq N-1},\ \ \{a_n\}_{n\in\mathbf{Z}_N},\ \text{where } a_n \in \mathbf{C}.$$

This means that a_n is uniquely determined for each $n \in \mathbf{Z}_N$. From this, a sequence can be viewed as a mapping from $\mathbf{Z}_N$ to $\mathbf{C}$. In the case that the range of the index set is obvious, we abbreviate the index set and simply write it as $\{a_n\}$.

Definition. A periodic autocorrelation function of $\{a_n\}_{n=0}^{N-1}$ is defined as follows;

$$ACF(\{a_n\}, l) = \sum_{m=0}^{N-l-1} a_{m+l}a_m^* + \sum_{m=N-l}^{N-1} a_{m+l-N}a_m^*.$$

Since $\mathbf{Z}_N$ is a complete representative system of $\mathbf{Z}/N\mathbf{Z}$, a sequence can be treated as a map from $\mathbf{Z}/N\mathbf{Z}$ to $\mathbf{C}$. So, a sequence can be described as $\{a_n\}_{n\in\mathbf{Z}/N\mathbf{Z}}$ [1] and an autocorrelation function $ACF(\{a_n\}, l)$ is expressed as follows;

$$ACF(\{a_n\}, l) = \sum_{m\in\mathbf{Z}/N\mathbf{Z}} a_{m+l}a_m^*.$$

Definition. A sequence $\{a_n\}_{n=0}^{N-1}$ is called perfect when its autocorrelation function is impulsive, that is, autocorrelation function $ACF(\{a_n\}, l)$ satisfies the following property.

$$ACF(\{a_n\}, l) \begin{cases} = 0 & \text{if } l \not\equiv 0 \mod N \\ \neq 0 & \text{if } l \equiv 0 \mod N \end{cases}$$

Definition. Let M be a positive integer. A sequence $\{a_n\}_{n=0}^{N-1}$ is called an M-phase sequence or a polyphase sequence of M-th root of unity, if ${a_n}^M = 1$ for all $n \in \mathbf{Z}_N$.

Definition. Let $\{a_n\}_{n=0}^{N-1}$ be a M-phase sequence, then a_n is given by ${\omega_M}^{f_n}$, where $f_n \in \mathbf{Z}/M\mathbf{Z}$. The sequence $\{f_n\}_{n=0}^{N-1}$ is called the exponent of $\{a_n\}_{n=0}^{N-1}$.

Using these words we describe the main theorem of the article.

Theorem 1 (main theorem)**.** Let p be an odd prime and $\{a_n\}_0^{p-1}$ be a p-phase seqence of length p with exponent $\{f_n\}_{n=0}^{p-1}$. Then the following two conditions are equivalent

(i) $\{a_n\}_{n=0}^{p-1}$ is perfect

(ii) f_n is quadratic polynomial in n

The proof of the theorem will be shown in the following section. After the proof, we describe the structure of the set of perfect polyphase sequence of odd prime length. The description is justified by the main theorem.

[1] Formally, we should write $a_{\overline{n}}$. But this style seems to be unsightly and we are convinced that the style written in the text will not cause confusion.

2 Proof of the main theorem

ω_p is abbreviated to ω. Generally, an equality in $\mathbf{Z}/p\mathbf{Z}$ should be represented as $m \equiv n \mod (p)$. Since there are a lot of equality in $\mathbf{Z}/p\mathbf{Z}$, in this section, we abbreviate $'' \mod (p)''$ and simply describe as $m \equiv n$ if there is no confusion.

Since (ii)$\Longrightarrow$ (i) is obvious, we focus on proving (i)$\Longrightarrow$(ii).

To handle f_n, we use the following lemma.

Lemma 1. Let p be an odd prime integer and f_n be an arbitrary elenet of $\mathbf{Z}/p\mathbf{Z}$. Then, there exists a polynomial $F(X) \in \mathbf{Z}[X]$ which satisfies that $F(n) \equiv f_n$ for all $n \in \mathbf{Z}/p\mathbf{Z}$ and the degree of $F(X)$ is $p-1$ or less.

The proof of the lemma is shown in the appendix.

According to the Lemma 1, there is a polynomial $F(X) \in \mathbf{Z}[X]$ such that

$$F(X) = \sum_{j=0}^{k} c_j X^j \quad c_k \neq 0, \qquad F(n) \equiv f_n,$$

where k is a degree of $F(X)$.

If $c_k \equiv 0$, we can retake$\displaystyle\sum_{j=0}^{k-1} c_j X^j$ as $F(X)$. By repeating this operation, we can assume that $c_k \not\equiv 0$. In the case of $k=2$, it is easy to show that the sequence $\{a_n\} = \{\omega^{F(n)}\}$ is a perfect polyphase sequence of length p, and in the case of $k=1$ or 0, it is obvious that the sequence $\{a_n\} = \{\omega^{F(n)}\}$ is not a perfect polyphase sequence of length p. Let us consider the case of $k \geq 3$.

Let $\theta(l)$ be an autocorrelation function of $\{a_n\}$, i.e.

$$\theta(l) = ACF(\{a_n\}, l) = \sum_{n \in \mathbf{Z}/p\mathbf{Z}} a_{n+l} a_n^* = \sum_n \omega^{F(n+l)-F(n)}$$

where $l \in \mathbf{Z}/p\mathbf{Z}$. $\theta(l)$ is expressed as a linear combination of $\omega^0 = 1, \omega^1, \omega^2, \cdots, \omega^{p-1}$ by non negative integer coefficients. If $\{a_n\}$ is perfect and polyphase, then

$$\theta(l) = \begin{cases} 0 & \text{if } l \not\equiv 0 \\ p & \text{if } l \equiv 0 \end{cases}$$

Suppose that $\sum_{j=0}^{p-1} b_j \omega^j = 0$, where $b_j \in \mathbf{Z}$. Since ω is a primitive p-th root of unity, all coefficients are same each other, i.e. $b_0 = b_1 = \cdots = b_{p-1}$. We find an equality of sets as follows;

$$\{\overline{G_l(0)}, \overline{G_l(1)}, \cdots, \overline{G_l(p-1)}\} = \{\overline{0}, \overline{1}, \cdots, \overline{(p-1)}\}$$

where $G_l(X) = F(X+l) - F(X)$. Then we obtain equalities in $\mathbf{Z}/p\mathbf{Z}$ as follows;

$$\sum_{n \in \mathbf{Z}/p\mathbf{Z}} G_l(n)^m \equiv \sum_{n \in \mathbf{Z}/p\mathbf{Z}} n^m \text{ for arbitrary } m.$$

To calculate the right hand side, we use the following lemma.

Lemma 2. Let p be an odd prime integer and d be a positive integer. We define a mapping B from $\mathbf{Z}$ to $\mathbf{Z}/p\mathbf{Z}$ as follows;

$$B(d) \equiv \sum_{n \in \mathbf{Z}/p\mathbf{Z}} n^d.$$

Then,

$$B(d) \equiv \begin{cases} -1 & \text{if } d \equiv 0 \mod (p-1) \\ 0 & \text{if } d \not\equiv 0 \mod (p-1) \end{cases}$$

The proof of the lemma is shown in the appendix.

According to Lemma 2, if $1 \leq m \leq p-2$, the right side is equal to 0, therefore,

$$\sum_{n \in \mathbf{Z}/p\mathbf{Z}} G_l(n)^m \equiv 0,$$

for all l and m such that $1 \leq l \leq p-1$ and $1 \leq m \leq p-2$. Based on the definition of $G_l(X)$, left hand side is calculated as follows;

$$\begin{aligned}\sum_{n \in \mathbf{Z}/p\mathbf{Z}} G_l(n)^m &\equiv \sum_{n \in \mathbf{Z}/p\mathbf{Z}} (F(n+l) - F(n))^m \\ &\equiv \sum_n \left(\sum_{j=0}^{k} c_j((n+l)^j - n^j) \right)^m .\end{aligned}$$

Since l is prime to p, $l^{p-1} \equiv 1$ and the mapping $n \equiv ly$ is a one to one mapping from $\mathbf{Z}/p\mathbf{Z}$ to $\mathbf{Z}/p\mathbf{Z}$ for each l. Therefore;

$$\begin{aligned}\sum_{n \in \mathbf{Z}/p\mathbf{Z}} G_l(n)^m &\equiv \sum_{y \in \mathbf{Z}/p\mathbf{Z}} \left(\sum_{j=1}^{k} c_j((ly+l)^j - (ly)^j) \right)^m \\ &\equiv \sum_y \prod_{\xi=1}^{m} \left(\sum_{j_\xi=1}^{k} c_{j_\xi}((y+1)^{j_\xi} - y^{j_\xi}) l^{j_\xi} \right) \\ &\equiv \sum_{j=0}^{p-2} A_{m,j} l^j \equiv 0,\end{aligned}$$

where

$$A_{m,j} \equiv \sum_y \sum_{\substack{1 \leq j_\xi \leq k \\ \sum j_\xi \equiv j \mod (p-1)}} \prod_{\xi=1}^{m} c_{j_\xi} \left((y+1)^{j_\xi} - y^{j_\xi} \right)$$

These equations are expressed as a system of linear equations as follows;

$$\begin{pmatrix} 1^0 & 1^1 & 1^2 & \cdots & 1^{p-2} \\ 2^0 & 2^1 & 2^2 & \cdots & 2^{p-2} \\ 3^0 & 3^1 & 3^2 & \cdots & 3^{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (p-1)^0 & (p-1)^1 & (p-1)^2 & \cdots & (p-1)^{p-2} \end{pmatrix} \begin{pmatrix} A_{m,0} \\ A_{m,1} \\ A_{m,2} \\ \vdots \\ A_{m,p-2} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

The matrix appeared in the left side is a Vandermonde matrix and it is easily shown that its determinant $\not\equiv 0$. Finally we obtained following equalities.

$$A_{m,j} \equiv 0, \tag{1}$$

for all m and j such that $1 \leq m \leq p-2$ and $0 \leq j \leq p-2$. We determine m according to k. It will be shown that a fact conflict with (1) occurs for such m if $k \geq 3$.

Let m_1 be the maximal integer which satisfies $km_1 < p$, i.e. m_1 is determined by the following inequalities;

$$km_1 < p < k(m_1 + 1).$$

Since $k \geq 3$, $2m_1 \leq \frac{2}{3}km_1 < \frac{2p}{3} \leq p-1$. So, $A_{2m_1,j} = 0$ for all j such that $0 \leq j \leq p-2$.

To calculate $A_{2m_1,j}$, let's consider the system of equations and inequalities of $j_1, j_2, \cdots, j_{2m_1}$ given by

$$\begin{cases} j_1 + j_2 + \cdots + j_{2m_1} \equiv j \quad \bmod (p-1) \\ 1 \leq j_1 \leq k \\ \cdots \\ 1 \leq j_{2m_1} \leq k \\ 0 \leq j \leq p-2 \end{cases} . \tag{2}$$

We take j such that the solution of (2) contains $(j_1, j_2, \cdots, j_{2m_1}) = (\underbrace{k, k, \cdots, k}_{2m_1})$.

Let's consider the case of $k \not|(p-1)$. Since $k \not|(p-1)$, $km_1 < p-1$. If $2km_1 \geq p-1$, set $j_0 = 2km_1 - p + 1$, otherwise set $j_0 = 2km_1$. Then, $0 \leq j \leq p-2$, so $A_{2m_1,j_0} \equiv 0$.

On the other hand, the solution of consists in $(j_1, j_2, \cdots, j_{2m_1}) = (k, k, \cdots, k)$ and positive integer solution of $j_1 + j_2 + \cdots + j_{2m_1} = j_0$. Since A_{2m_1,j_0} is a sum of terms corresponding to the solution, A_{2m_1,j_0} is expressed as follows;

$$\begin{aligned} A_{2m_1,j_0} \equiv \; & {c_k}^{2m_1} \sum_y ((y+1)^k - y^k)^{2m_1} \\ & + \sum_y \sum_{\substack{1 \leq j_1, \cdots, j_{2m_1} \leq k \\ \sum j_\xi = j_0}} c_{j_1} \cdots c_{j_{2m_1}} \prod_{\xi=1}^{2m_1} ((y+1)^{j_\xi} - y^{j_\xi}). \end{aligned}$$

To calculate the second term, we evaluate the degree of the polynomial in y inside of $\sum_y$ of it. Since the degree $= \sum_{\xi=1}^{2m_1}(j_\xi - 1) = j_0 - 2m_1 < p-1$ the second term is equal to 0 because of the Lemma 2. To calculate the first term, we use the following lemma.

Lemma 3. Suppose that k is an integer such that $k \geq 3$. Let m_1 be an integer which satisfies $km_1 < p < k(m_1+1)$. Then,

$$\sum_{y\in\mathbf{Z}/p\mathbf{Z}} \left((y+1)^k - y^k\right)^{2m_1} \equiv \begin{cases} (-1)^{m_1+1}{}_{2m_1}C_{m_1} \cdot {}_{km_1}C_{p-1-km_1} & \text{if } k \not| (p-1) \\ (-1)^{m_1+1}{}_{2m_1}C_{m_1} & \text{if } k|(p-1) \end{cases}$$

The proof of the lemma is shown in the appendix.

Finally,

$$A_{2m_1,j_0} \equiv (-1)^{m_1+1}{c_k}^{2m_1}{}_{2m_1}C_{m_1} \cdot {}_{km_1}C_{p-1-km_1}$$

Since $2m_1 < km_1 < p$, ${}_{2m_1}C_{m_1} \not\equiv 0$ and ${}_{km_1}C_{p-1-km_1} \not\equiv 0$. This contradicts the equation (1).

Next, we treat the case of $k|(p-1)$. Since $k|(p-1)$, $km_1 = p-1$. We consider $j=0$. Since maximal value of $j_1 + \cdots + j_{2m_1}$ is $2km_1 = 2(p-1)$, Then, the solution of (2) consists in $(j_1, j_2, \cdots, j_{2m_1}) = (k, k, \cdots, k)$ and positive integer solution of $j_1 + j_2 + \cdots + j_{2m_1} = p-1$. Since $A_{2m_1,0}$ is a sum of terms corresponding to the solution, it is expressed as follows;

$$\begin{aligned} A_{2m_1,0} \equiv\ & {c_k}^{2m_1}\sum_y((y+1)^k - y^k)^{2m_1} \\ & + \sum_y \sum_{\substack{1\leq j_1,\cdots,j_{2m_1}\leq k \\ \sum j_\xi = p-1}} c_{j_1}\cdots c_{j_{2m_1}} \prod_{\xi=1}^{2m_1}((y+1)^{j_\xi} - y^{j_\xi}). \end{aligned}$$

By the similar dicussion, it is shown that the second term $\equiv 0$. To calculate the first term, we use Lemma 3.

Finally,

$$A_{2m_1,0} \equiv (-1)^{m_1+1}{c_k}^{2m_1}{}_{2m_1}C_{m_1}$$

Since $2m_1 < km_1 = p-1$,$(2m_1)! \not\equiv 0$. Therefore, $A_{2m_1,0} \not\equiv 0$. This contradicts the equation (1).

The above logic shows that there exist $\alpha, \beta, \gamma \in \mathbf{Z}$ such that $a_n = \omega^{\alpha n^2 + \beta n + \gamma}$. It is clear that $\{\omega^{\beta n+\gamma}\}$ is not perfect.

This completes the proof of the theorem. □

3 Transformations of the set of the perfect polyphase sequences

Let N be a positive integer. Let S_N be the set of sequences of length N and P_N be the set of the perfect polyphase sequences of length N. Let $\omega = e^{\frac{2\pi i}{N}}$ be a primitive N-th root of unity. Let $K = \mathbf{Q}(\omega)$ be N-cyclotomic field, i.e. the field extension of $\mathbf{Q}$ by ω. We define transformations of P_N, which is described as ρ, σ, and τ. In the case that the length of sequences is odd prime, it will be shown that the transformation group generated by ρ, σ and τ, acts P_N transitively.

Theorem 2. Let r, s_1, s_2, t_1, t_2 be integers such that $r, s_1 \in \mathbf{Z}_N^\times$ and $s_2, t_1, t_2 \in \mathbf{Z}_N$. That is, r and s_1 are relatively prime to N, and s_2,t_1 and t_2 have no such restrictions. Let $\{a_n\}_{n=0}^{N-1}$ be an element of P_N . We define the mappings $\rho_r, \sigma_{(s_1,s_2)}$ and $\tau_{(t_1,t_2)}$ from P_N to S_N, as follows;

$$\begin{aligned} \rho_r(\{a_n\}_{n=0}^{N-1}) &= \{(a_n)^r\}_{n=0}^{N-1} \\ \sigma_{(s_1,s_2)}(\{a_n\}_{n=0}^{N-1}) &= \{a_{s_1 n+s_2}\}_{n=0}^{N-1} \\ \tau_{(t_1,t_2)}(\{a_n\}_{n=0}^{N-1}) &= \{\omega^{t_1 n+t_2} \cdot a_n\}_{n=0}^{N-1}, \end{aligned}$$

where $\omega = e^{\frac{2\pi i}{N}}$. Then, these mappings are bijective transformation of P_N .

Proof. It is obvious that the images of the mappings consist of the sequences of the power of ω, i.e. they are polyphase sequences of N-th root of unity.

For the proof of ρ_r, set $b_n = (a_n)^r$. Since r is relatively prime to N, the mapping $\omega \longmapsto \omega^r$ induces the homomorphism of K[8]. Let ϕ_r be this induced homomorphism. Then, an autocorrelation function of $\{b_n\}$ is calculated as follows;

$$\begin{aligned} ACF(\{b_n\}, l) &= \sum_{n=0}^{N-1} b_{n+l} {b_n}^* = \sum_{n=0}^{N-1} \frac{b_{n+l}}{b_n} \\ &= \sum_{n=0}^{N-1} \left(\frac{a_{n+l}}{a_n}\right)^r = \phi_r\left(\sum_{n=0}^{N-1} \frac{a_{n+l}}{a_n}\right) = \phi_r(ACF(\{a_n\}, l)) \end{aligned}$$

This shows that $\{b_n\}$ is perfect if $\{a_n\}$ is perfect.

For the proof of $\sigma_{(s_1,s_2)}$, set $b_n = a_{s_1 n+s_2}$, then

$$ACF(\{b_n\}, l) = \sum_{n=0}^{N-1} b_{n+l} {b_n}^* = \sum_{n=0}^{N-1} \frac{b_{n+l}}{b_n} = \sum_{n=0}^{N-1} \frac{a_{s_1(n+l)+s_2}}{a_{s_1 n+s_2}} = \sum_{n=0}^{N-1} \frac{a_{(s_1 n+s_2)+s_1 l}}{a_{s_1 n+s_2}}$$

Since s_1 is relatively prime to N, the mapping $n' = s_1 n + s_2$ is a bijective mapping on $\mathbf{Z}/N\mathbf{Z}$, therefore,

$$ACF(\{b_n\}, l) = \sum_{n'=0}^{N-1} \frac{a_{n'+s_1 l}}{a_{n'}} = ACF(\{a_n\}, s_1 l)$$

This shows that $\{b_n\}$ is perfect if $\{a_n\}$ is perfect.

For the proof of τ_{t_1,t_2}, set $b_n = \omega^{t_1 n+t_2} a_n$, then

$$\begin{aligned} ACF(\{b_n\}, l) &= \sum_{n=0}^{N-1} b_{n+l} {b_n}^* = \sum_{n=0}^{N-1} \frac{b_{n+l}}{b_n} = \sum_{n=0}^{N-1} \frac{\omega^{t_1(n+l)+t_2} a_{n+l}}{\omega^{t_1 n+t_2} a_n} \\ &= \omega^{t_1 l} \sum_{n=0}^{N-1} \frac{a_{n+l}}{a_n} = \omega^{t_1 l} ACF(\{a_n\}, l) \end{aligned}$$

Since $\omega^{t_1 l} \neq 0$, this shows that $\{b_n\}$ is perfect if $\{a_n\}$ is perfect.

It is easy to show the following equalities,

$$\rho_r \circ \rho_{r'} = \rho_{rr'} \quad \sigma_{(s_1,s_2)} \circ \sigma_{(s'_1,s'_2)} = \sigma_{(s'_1 s_1, s'_1 s_2+s'_2)} \quad \tau_{(t_1,t_2)} \circ \tau_{(t'_1,t'_2)} = \tau_{(t_1+t'_1, t_2+t'_2)}$$

where $\circ$ is a composition of the mappings. Since $\rho_1 = \sigma_{(1,0)} = \tau_{(0,0)} = id_{P_N}$ (the identity mapping of P_N), all of these mappings are bijective transformations of P_N. □ □

Let G be a transformation group of P_N. Since P_N is finite, G is a finite group. Let G_0 be a subgroup of G, generated by $\rho_r, \sigma_{(s_1,s_2)}, \tau_{(t_1,t_2)}$, where $r, s_1 \in \mathbf{Z}_N^\times$ and $s_2, t_1, t_2 \in \mathbf{Z}_N$.

Theorem 3. Suppose that N is odd prime and set $N = p$. G_0 acts on P_p transitively. In other words, there is only one point in the quotient space P_p/G_0, i.e. $|P_p/G_0| = 1$. More specifically, for arbitrary element $\{a_n\}_{n=0}^{p-1} \in P_p$, there exists an element $\chi \in G_0$ such that

$$\chi(\{a_n\}_{n=0}^{p-1}) = \left\{\omega^{n^2}\right\}_{n=0}^{p-1}$$

where $\omega = e^{\frac{2\pi i}{p}}$.

Proof. According to the theorem of the previous section, there exists $\alpha \in \mathbf{Z}_p^\times$ and $\beta, \gamma \in \mathbf{Z}_p$ such that

$$a_n = \omega^{\alpha n^2+\beta n+\gamma}$$

Since $[\alpha, p] = 1$, there exists $\alpha' \in \mathbf{Z}_N^\times$ such that $\alpha\alpha' \equiv 1 \mod p$. Then

$$(a_n)^{\alpha'} = \omega^{n^2+\alpha'\beta n+\alpha'\gamma}$$

Since $[2, p] = 1$, there exists $\beta' \in \mathbf{Z}_N$ such that $-2\beta' \equiv \alpha'\beta \mod p$. Then

$$(a_n)^{\alpha'} = \omega^{(n-\beta')^2+\alpha'\gamma-\beta'^2}$$

Set $\gamma' = \beta'^2 - \alpha'\gamma$, then

$$(\tau_{(0,\gamma')} \circ \sigma_{(1,\beta')} \circ \rho_{\alpha'})(\{a_n\}) = \left\{\omega^{n^2}\right\}$$

□ □

Chu sequences are famous perfect polyphase sequences [1, 3]. Let p be an odd prime number and $\{a_n\}_{n=0}^{p-1}$ be a Chu sequence of p. a_n is expressed as follows;

$$a_n = e^{\frac{\pi i}{p} rn(n+1)}, \text{ where } [r,p]=1$$

Since the coefficients of n^2 is not $\frac{2\pi ir}{p}$ but $\frac{\pi ir}{p}$, this expression looks slightly different from our result. But there exist $r' \in \mathbf{Z}_p^\times$ such that $rr' \equiv 2 \mod p$. Therefore,

$$(\tau_{(-2r',0)} \circ \rho_{r'})(\{a_n\}) = \{\omega^{-2r'n} \cdot e^{\frac{\pi i}{p} rr'n(n+1)}\} = \left\{\omega^{n^2}\right\}$$

4 Concluding remarks

A parameterization of the set of perfect polyphase sequence denoted by P_p was obtained and transitivity of the action of G_0 on P_p was proved.

Let $\{a_n\}_{n=0}^{p-1} \in P_p$ be an arbitrary perfect polyphase sequence of odd prime length p. It was shown that there exist $\alpha \in \mathbf{Z}_N^\times, \beta, \gamma \in \mathbf{Z}_N$ such that $a_n = \omega^{\alpha n^2+\beta n+\gamma}$, where ω is a p-th root of unity. The proof consists in several steps;

- Since $\{a_n\}$ is polyphase, we can find a mapping $f : \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{Z}/p\mathbf{Z}$ such that $a_n = \omega^{f(n)}$.
- Find a polynomial $F(X) \in \mathbf{Z}[X]$ such that $f(n) \equiv F(n) \mod p$
- Obtain the equalities of coefficients of $F(X)$ from perfectness of $\{a_n\}$.
- These equalities contradict that the degree of $F(X)$ is equal to three or more.

We defined transformations of P_p, which was described as $\rho_r, \sigma_{(s_1,s_2)}$, and $\tau_{(t_1,t_2)}$. Let G_0 be a subgroup of the transformation group of P_p, generated by them. It was shown that for an arbitrary sequence $\{a_n\}_{n=0}^{p-1} \in P_p$ (including Chu sequence), there exists an element $\chi \in G_0$ such that

$$\chi(\{a_n\}_{n=0}^{p-1}) = \{\omega^{n^2}\}_{n=0}^{p-1}$$

For future research, we would like to point out the definition of polyphase sequence. We defined that $\{a_n\} \in \mathbf{S}_N$ is polyphase if and only if "$a_n^N = 1$ for all n". According to the result obtained by Gabidulin[7], "There are only finitely many perfect auto-correlation polyphase sequences of prime length." His intention is that there exist infinitely many perfect polyphase sequences for each prime but there exit finitely many essentially different perfect polyphase sequence for each prime. He defined that the polyphase sequence is a sequence whose components are on the unit disk in $\mathbf{C}$. Though e^i is on the unit disk, there exists no integer N_0 such that $(e^i)^{N_0} = 1$. From this point, we think that the definition would be corrected. We think that the following expanded definition is natural; "there exist an integer N_0 such that $a_n^{N_0} = 1$ for all n" Though we adopt such expanded definition of polyphase sequences, following proposition may be proved.

Conjecture. Let $\tilde{P}_p$ be the set of perfect polyphase sequence of odd prime length p in the meaning of the expanded definition. Let $\{a_n\}_{n=0}^{p-1} \in \tilde{P}_p$ There exist $\alpha \in \mathbf{Z}_p^{\times}, \beta', \gamma' \in \mathbf{Q}$ such that

$$a_n = \omega^{\alpha n^2 + \beta' n + \gamma'}, 0 \leq \beta', \gamma' < 1,$$

where $\omega = e^{\frac{2\pi i}{p}}$.

Of course the inverse of the conjecture is easily shown, i.e. it is easy to show that if $\alpha \in \mathbf{Z}_p^{\times}, \beta', \gamma' \in \mathbf{Q}$, then $\{\omega^{\alpha n^2 + \beta' n + \gamma'}\} \in \tilde{P}_p$. It is also easy to show the following theorem.

Theorem 4. Let $u_1, u_2 \in \mathbf{Q}$ be rational numbers. $\tilde{\tau}_{(u_1,u_2)}$ is a transformation of $\tilde{P}_p$ defined as follows;

$$\tilde{\tau}_{(u_1,u_2)}(\{\tilde{a}_n\}) = \{\omega^{u_1 n + u_2} \cdot \tilde{a}_n\}.$$

where $\omega = e^{\frac{2\pi i}{p}}$. Then, $\tilde{\tau}_{(u_1,u_2)}$ is a bijective mapping of $\tilde{P}_p$

Let $\tilde{G}_1$ be transformation group generated by $\tilde{\tau}_{(u_1,u_2)}$. If the conjecture is correct, it is easily proved that the quotient space $\tilde{P}_p/\tilde{G}_1$ is a finite set although $\tilde{P}_p$ is not a finite set. More specifically, the following proposition can be easily proved.

Conjecture. There are $p-1$ points in the quotient space $\tilde{P}_p/\tilde{G}_1$, i.e. $|\tilde{P}_p/\tilde{G}_1| = p-1$.

5 Appendix

As an appendix to the article, proofs of the lemmata are described.

5.1 Proof of Lemma 1

Let k be an integer such that $1 \leq k \leq p-1$. We define the polynomials $D_k(X) \in \mathbf{Z}[X]$ for each k as follows;

$$D_k(X) \quad = \quad - \prod_{\substack{l \neq k \\ 0 \leq l \leq p-1}} (X - l)$$

$D_k(X)$ is a polynomial of which the degree is $(p-1)$ and coefficients are integers, and satisfies the following equalities;

$$\begin{cases} D_k(j) \equiv 0 & \text{for } 1 \leq j \leq k-1 \text{ or } k+1 \leq j \leq p-1 \\ D_k(k) \equiv 1 \end{cases}$$

Let $f(n)$ be given by $f(n) \equiv \overline{r_n}$ arbitrarily. Set $F(X)$ as follows;

$$F(X) = \sum_{k=0}^{p-1} r_k D_k(X)$$

It is obvious that $F(n) \equiv r_n$ for all $0 \leq n \leq p-1$ and the degree of $F(X)$ is $p-1$ or less. This completes the proof of Lemma 1. □

5.2 Proof of Lemma 2

Suppose that $1 \leq d \leq p-1$. Let X be an indefinite element and consider binomial expansion of $(X+1)^{d+1}$.

$$(X+1)^{d+1} = X^{d+1} +_{d+1} C_d X^d +_{d+1} C_{d-1} X^{d-1} \cdots +_{d+1} C_1 X^1 + 1$$

Consider the case of $X = 1, 2, \cdots, p$ and calculate the sum.

$$(p+1)^{d+1} - 1 - p =_{d+1} C_d \sum_{X=1}^{p} X^d +_{d+1} C_{d-1} \sum_{X=1}^{p} X^{d-1} \cdots +_{d+1} C_1 \sum_{X=1}^{p} X^1$$

This equality is transformed to the equality of $\mathbf{Z}/p\mathbf{Z}$, i.e.

$${}_{d+1}C_d B(d) +_{d+1} C_{d-1} B(d-1) \cdots +_{d+1} C_1 B(1) \equiv 0$$

If $d \leq p-2$, the following equality holds for j such that $0 \leq j \leq d+1$,

$${}_{d+1}C_j \not\equiv 0$$

Then, $B(d) \equiv 0$ is concluded inductively.

Let $x \in \mathbf{Z}/p\mathbf{Z}$. If $x \not\equiv 0$, $x^{p-1} \equiv 1$. Therefore,

$$B(p-1) \equiv \sum_{x \in \mathbf{Z}/p\mathbf{Z}} x^{p-1} \equiv 0^{p-1} + \underbrace{1 + 1 + \cdots + 1}_{p-1} \equiv -1$$

Since $x^p \equiv x$ for all $x \in \mathbf{Z}/p\mathbf{Z}$, it is obvious that $B(d) \equiv B(d-p+1)$ for $d \geq p$. Then, we reach the general case. □

5.3 Proof of Lemma 3

To calculate the sum, we use the binomial expansion.

$$\begin{aligned} \sum_y ((y+1)^k - y^k)^{2m_1} &\equiv \sum_y \sum_{j=0}^{2m_1} {}_{2m_1}C_j (-1)^j (y+1)^{kj} (y^k)^{2m_1 - j} \\ &\equiv U + V + W, \end{aligned}$$

where

$$\begin{aligned} U &\equiv \sum_y \sum_{j=0}^{m_1 - 1} {}_{2m_1}C_j (-1)^j (y+1)^{kj} (y^k)^{2m_1 - j}, \\ V &\equiv \sum_y {}_{2m_1}C_{m_1} (-1)^{m_1} (y+1)^{km_1} (y^k)^{2m_1 - m_1}, \\ W &\equiv \sum_y \sum_{j=m_1+1}^{2m_1} {}_{2m_1}C_j (-1)^j (y+1)^{kj} (y^k)^{2m_1 - j}. \end{aligned}$$

By changing variables, $j = 2m_1 - j', y = -1 - y'$, W is transformed as follows.

$$\begin{aligned} W &\equiv \sum_{y'} \sum_{j'=0}^{m_1-1} {}_{2m_1}C_{2m_1-j'}(-1)^{2m_1-j'}(-y')^{k(2m_1-j')}((-1-y')^k)^{j'} \\ &\equiv \sum_{y'} \sum_{j'=0}^{m_1-1} {}_{2m_1}C_{j'}(-1)^{-j'-kj'+kj'}(y')^{k(2m_1-j')}(1+y')^{kj'} \\ &\equiv U \end{aligned}$$

5.3.1 in the case of $k \not| (p-1)$

Let us consider U. Since $k \not| (p-1)$, $km_1 < p-1$. Since $0 \le j \le m_1 - 1$, $(y+1)^{kj} y^{k(2m_1-j)}$ is a polynomial in y of degree $2km_1$ and its degree is evaluated as follows;

$$2p-2 > 2km_1 > 2p-2k > 2p-2\frac{p-1}{2} = p+1.$$

The degree of the lowest term is $k(2m_1-j)$ and is evaluated as follows;

$$k(2m_1-j) \ge k(2m_1-(m_1-1)) = k(m_1+1) > p.$$

So the degree of each term is bigger than $p-1$ and smaller than $2(p-1)$, i.e. $U = W = 0$ because of Lemma 2.

$$\begin{aligned} \sum_{y \in \mathbf{Z}/p\mathbf{Z}} \left((y+1)^k - y^k)\right)^{m_1} &\equiv {}_{2m_1}C_{m_1}(-1)^{m_1} \sum_y (y+1)^{km_1} y^{km_1} \\ &\equiv {}_{2m_1}C_{m_1}(-1)^{m_1} \sum_y \sum_{j=0}^{km_1} {}_{km_1}C_j y^{j+km_1} \end{aligned}$$

Since $p-1-km_1 < p-1-k\left(\frac{p}{k}-1\right) = k-1 \le km_1$ and $p-1-km_1 > p-1-p = -1$, j which satifies $j + km_1 = p-1$ is uniquely determined in the range of $0 \le j \le km_1$. Therefore

$$\sum_{y \in \mathbf{Z}/p\mathbf{Z}} \left((y+1)^k - y^k)\right)^{m_1} \equiv {}_{2m_1}C_{m_1}(-1)^{m_1} {}_{km_1}C_{p-1-km_1}(-1)$$

5.3.2 in the case of $k|(p-1)$

Let us consider V. Since $y^{p-1} \equiv 1$ for $y \not\equiv 0$ in $\mathbf{Z}/p\mathbf{Z}$,

$$\begin{aligned} V &\equiv {}_{2m_1}C_{m_1}(-1)^{m_1} \sum_y (y+1)^{km_1} y^{km_1} \\ &\equiv {}_{2m_1}C_{m_1}(-1)^{m_1} \sum_{y \not\equiv 0,-1} (y(y+1))^{km_1} \\ &\equiv -2 \, {}_{2m_1}C_{m_1}(-1)^{m_1} \end{aligned}$$

Let us consider U. Since $k|(p-1)$, $km_1 = p-1$. Since $0 \leq j \leq m_1 - 1$, $(y+1)^{kj}y^{k(2m_1-j)}$ is a polynomial in y of degree $2km_1 = 2(p-1)$ and the degree of the lowest term is $k(2m_1 - j)$ and is evaluated as follows;

$$k(2m_1 - j) \geq k(2m_1 - (m_1 - 1)) = k(m_1 + 1) > p.$$

Since the terms whose degree are not $2p-2$ are 0 by the summation of y, U is calculated as follows;

$$U \equiv \sum_{j=0}^{m_1-1} {}_{2m_1}C_j (-1)^j \sum_y y^{2p-2} \equiv -\sum_{j=0}^{m_1-1} {}_{2m_1}C_j (-1)^j$$

By changing $j = 2m_1 - j'$,

$$W \equiv -\sum_{j'=m_1+1}^{2m_1} {}_{2m_1}C_{2m_1-j'} (-1)^{2m_1-j'} \equiv -\sum_{j'=m_1+1}^{2m_1} {}_{2m_1}C_{j'} (-1)^{j'}$$

Therefore,

$$\begin{aligned} U+V+W &\equiv -\sum_{j=0}^{m_1-1} {}_{2m_1}C_j (-1)^j - 2\ {}_{2m_1}C_{m_1} (-1)^{m_1} - \sum_{j=m_1+1}^{2m_1} {}_{2m_1}C_j (-1)^j \\ &\equiv -(1-1)^{2m_1} - {}_{2m_1}C_{m_1} (-1)^{m_1} \\ &\equiv -{}_{2m_1}C_{m_1} (-1)^{m_1} \end{aligned}$$

$$\therefore \sum_{y \in \mathbf{Z}/N\mathbf{Z}} \left((y+1)^k - y^k\right)^{m_1} \equiv (-1)^{m_1+1}\ {}_{2m_1}C_{m_1}$$

References

[1] P.Z. Fan, and M. Darnell, "Sequence design for communications applications," (Reseach Studies Press, London, 1996)

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

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

[4] 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, 2014.

[5] K.H. Park, H.Y. Song, D.S. Kim, and S.W. Golomb, "Optimal Families of Perfect Polyphase Sequences From the Array Structure of Fermat-Quotient Sequences," IEEE Trans. Inf. Theory, vol. 62, no. 2, pp. 1076–1086, 2016.

[6] W.H. Mow, “A new unified construction of perfect root-of-unity sequences,” Proceedings of ISSSTA’95 International Symposium on Spread Spectrum Techniques and Applications, Mainz, Germany, 1996, pp. 955-959 vol.3.

[7] E. M. Gabidulin, “There are only finitely many perfect auto-correlation polyphase sequences of prime length,” Proceedings of 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, 1994, pp. 282-282.

[8] S. Lang, “Algebra (Graduate TExts in Mathematics 211),” (Springer, USA, 2005)

[9] T. Maeda and T. Hayashi, “Fourier Analysis of Sequences over a Composition Algebra over the Real Number Field,” IEICE Trans. Fund., vol.E96-A, no.12, pp.2452–2456, December 2013.

[10] T. Maeda and Y. Watanabe and T. Hayashi, “Parameterization of Higher-Dimensional Perfect Sequences over a Composition Algebra over $\mathbb{R}$,” IEICE Trans. Fund., vol.E98-A, no.12, pp.2439–2445, December 2015.