creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

Perfectness of the Fermat-quotient Sequences

Ki-Hyeon Park

The Graduate School

Yonsei University

Department of Electrical and Electronic Engineering

Perfectness of the Fermat-quotient Sequences

by

Ki-Hyeon Park

A Dissertation Submitted to the

Graduate School of Yonsei University

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

Supervised by

Professor Hong-Yeop Song, Ph.D.

Department of Electrical and Electronic Engineering
The Graduate School

YONSEI University

December 2015

This certifies that the dissertation of
Ki-Hyeon Park is approved.

Thesis Supervisor: Hong-Yeop Song

Jong-Soo Seo

Kwang Soon Kim

Sooyong Choi

Habong Chung

The Graduate School
Yonsei University
December 2015

감사의 글

10년에 이르렀던 기나긴 수학 과정 동안 정말 많은 일이 있었습니다. 그 중에는 기쁜 일, 보람된 일도 많았고, 힘든 일이나 고민, 절망도 없다고는 할 수 없었지만 지금 돌이켜 보면 그 경험들 모두가 저에게 있어 그 이전의 저보다 한 걸음 더 성숙할 수 있는 소중한 토대들이 되어 주었습니다. 그 시간 동안 이 조그만 페이지에 모두 적을 수 없을 만큼 너무나 많은 사람들에게 도움을 받았고, 그 분들께 모두 감사 인사를 적기는 어렵지만, 그래도 이 커다란 마침표를 찍을 수 있기 위해 이끌어 주신 분들께 약소하게나마 이 자리를 빌어 감사의 글을 드리고자 합니다.

먼저 결코 짧지 않았던 학위 과정 동안 부족하고 천덕꾸러기였던 저를 끊임없이 지도해 주시고 부족한 점을 채워 주시면서 박사학위까지 이끌어 주신 우리 지도교수님인 송홍엽 교수님께 가장 큰 감사를 드리고 싶습니다.

그리고 이 학위논문을 완성하는 데 아낌없는 조언과 격려를 주셨던 서종수 교수님, 정하봉 교수님, 김광순 교수님, 그리고 최수용 교수님께도 큰 감사를 드립니다. 그리고 학위 과정 중 저에게 소중한 가르침과 조언을 주셨던 다른 교수님들께도 감사를 드리고 싶습니다.

또한 긴 연구실 생활 동안 서로 돕고 의지하며 연구활동을 같이 해 나간 동료와 선, 후배들에게도 감사 인사를 하고 싶습니다. 아무것도 모르는 풋내기 시절부터 많은 도움을 주신 홍윤표, 김영준, 김준성, 김대선, 진석용, 김주영, 김성하, 유장헌, 김태의, 백종민, 오현영, 박선영, 그리고 김정현 선배, 그리고 서로 의지하고 많은 도움을 주고받았던 미영누나, 진수, 석민이, 영태, 민규, 경군이, 인선이, 그리고 다빈이에게도 이 자리를 빌어 감사의 글을 전합니다. 소중한 연구 환경과 노하우의 토대를 만들어 주신 이전 선배들과 앞으로 연구실에 참여하고 이끌어나갈 후배들에게도 감사의 글을 전하려고 합니다.

마지막으로, 기나긴 수학 과정을 말없이 지지해 주시고 뒷바라지해 주시면서 말로 다 하기 힘들 만큼 많은 힘이 되어 주신 어머님, 아버님께 가장 큰 감사를 드리며 그 모든 분들께 이 논문을 바칩니다.

2015년 12월

박기현 드림

Contents

List of Figures **iii**

List of Tables **iv**

Abstract **v**

1 Introduction **1**

1.1 Motivation 1

1.1.1 Fermat-quotient Sequences 2

1.1.2 Nonbinary Sequence Families with Optimal Correlation 4

1.2 Overview 8

2 Perfectness of the Fermat-quotient Sequences **11**

2.1 The p-ary Fermat-quotient Sequence of period p^2 and its Properties . . 11

2.1.1 Difference Sequences and RC-Balancedness 12

2.1.2 Transformations of Sequences Preserving RC-Balancedness . . 14

2.2 Generalized Optimal Families from Fermat-quotient Sequences 17

2.3 Relations with Frank-Zadoff Sequences 22

3 Optimal Families of Perfect Polyphase Sequences **24**

3.1 Optimal Generators 24

3.1.1 Generators and Optimal Families 26

3.1.2 Perfect Generators 30

3.1.3 Optimal Generators 32

3.2 Counting the Number of Families 47

3.3 Applications to LPI Signal Design 50

4 Numerical Results and Concluding Remarks **56**

Bibliography **58**

Abstract (in Korean) **68**

List of Figures

3.1 Relation of transforms between generators and members of their associated families 43

4.1 Hierarchy of p-ary perfect sequences of period p^2 59

List of Tables

2.1 The Fermat-quotient sequence and its transforms for $p = 5$. Here, $\sigma = (043)$ in cycle notation. 17

2.2 Example of optimal families from the Fermat-quotient sequence for $p = 5$. 21

4.1 List of all the inequivalent optimal generators for $p \leq 13$ and their representations of the form $\mathbf{g}[p, \kappa, 1, 0]$ 57

ABSTRACT

Perfectness of the Fermat-quotient Sequences

Ki-Hyeon Park
Department of Electrical and Electronic Eng.
The Graduate School
Yonsei University

In this dissertation, 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 sequences. We propose a collection of 'optimal' families of perfect polyphase sequences using 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 Fermat-quotient

sequences or from Frank-Zadoff sequences, but some families are NEW for $p \geq 11$. We also show that the proposed method has a far larger design space than previous methods.

Key words : Fermat-quotient sequences, Frank-Zadoff sequences, Perfect polyphase sequences, Generators of perfect sequences, Optimal family of perfect sequences, Transformations of perfect sequences.

Chapter 1

Introduction

1.1 Motivation

Sequences with good correlation characteristics have been widely studied for their application to various communication systems [1–18]. For example, the systems using the direct-sequence spread-spectrum 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 robust anti-jamming capability [19].

Recent applications include such commercial mobile communication systems as CDMA, WCDMA, and 3GPP LTE [20, 21] and global navigation satellite systems as GPS [22] and GALILEO [23], in which not only a single sequence with good autocorrelation characteristics but also a family of sequences with good cross-correlation characteristics play an essential role in their performance. Non-binary sequences with good correlation characteristics also find applications to the pulse-compression RADAR or active SONAR [24–26]. 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 [5, 27–30].

In this dissertation, we introduce new families of sequences with optimal periodic correlation property from the well-known Fermat quotients, and propose methods to generate much more different families preserving the correlation property.

1.1.1 Fermat-quotient Sequences

The Fermat quotients have been studied extensively because of its numerous characteristics and properties in number theory [31–37]. 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 [32, 36] showed some randomness properties, and Ostafe [34] studied dynamical systems using Fermat quotients, and proposed its application to the communication and cryptography systems. Fermat quotients and derived binary sequences are generalized to Euler quotients [37]. Some recent result of Su can be found in [35], who designed a practical sequence families from the p-ary Fermat-quotient sequences, showing their Hamming correlation property [38] for frequency-hopping spread spectrum systems [39, 40], and those of Gomez and Winterhof [33] estimating the multiplicative character sums of the p-ary Fermat-quotient sequences.

The definition of Fermat quotient sequence is shown below:

Definition 1.1 [31–33, 36] Let p be an odd prime and

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

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

$$q(t) \equiv \begin{cases} Q(t) \pmod{p} & \text{if} \quad t \not\equiv 0 \pmod{p}, \\ 0 \pmod{p} & \text{otherwise.} \end{cases} \tag{1.1}$$

□

Example 1.1 When $p = 3$, $q(0) = 0$, $q(1) = \frac{1^2-1}{3} = 0$, $q(2) = \frac{2^2-1}{3} = 1$, $q(3) = 0$, $q(4) = \frac{4^2-1}{3} = 5 \equiv 2 \pmod 3$, $q(5) = \frac{5^2-1}{3} = 8 \equiv 2 \pmod 3$, $q(6) = 0$, $q(7) = \frac{7^2-1}{3} \equiv 1 \pmod 3$, $q(8) = \frac{8^2-1}{3} \equiv 0 \pmod 3$, and so on. Therefore,

$$\mathbf{q} = (0, 0, 1, 0, 2, 2, 0, 1, 0, \ldots).$$

□

The following properties of Fermat-quotient sequences are well-known [31–33, 36].

Lemma 1.1 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 1.1 can be seen very easily when we write the sequence $\mathbf{q}$ as an array of size $p \times p$:

$$\mathbf{q} = \begin{bmatrix} q(0) & q(1) & \cdots & q(p-1) \\ q(p) & q(p+1) & \cdots & q(2p-1) \\ q(2p) & q(2p+1) & \cdots & q(3p-1) \\ \vdots & \vdots & \ddots & \vdots \\ q((p-1)p) & q((p-1)p+1) & \cdots & q(p^2-1) \end{bmatrix} \tag{1.2}$$

The third item of Lemma 1.1 implies that every column (except for the left-most one) is balanced. In other word, any of them contains all the symbols from 0 to $p-1$ exactly the same number.

1.1.2 Nonbinary Sequence Families with Optimal Correlation

The most common examples of the non-binary sequences are the polyphase sequences which have values on the unit circle of the complex plane. These polyphase sequences having complex values with a constant unit amplitude have been widely studied to make sequences with the perfect periodic autocorrelation, and to design phase-coded pulses for pulse-compression [41–43]. Heimiller [9] 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 thesis), 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, which is called Frank-Zadoff sequences [10]. This had been the only perfect sequence until Chu proposed in 1972 another type: N-ary 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 in 1992 by Popovic [12], and this generalized version was recently adopted to 3GPP LTE standard, which is now called Zadoff-Chu sequences [20, page 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 length m^{2k+1} over m^{k+1}-phases in 1983 [44]. These ideas have been generalized for using smaller number of alphabet size by Liu and Fan [45] in 2004 as well as by Blake and Tirkel [46] in 2014.

In 1993, Zhang and Golomb [5] 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 [16] in 1985 and Mow unified the constructions of perfect polyphase sequences [17]. Recently, in 2014, Soltanalian and Stoica [18] studied these problems and considered their existence from Mow's results as well as some results of analysis using relative difference sets [47].

In 1988, the cross-correlation of original Frank-Zadoff sequence was studied by Suehiro and Hatori [2]. They showed that the sequence family has also optimal cross-correlation in the sense of the lower bound of Sarwate [13] (we will call this 'optimal family' in this thesis). In 1993, Gabidulin [48] 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 was studied by Popovic [12] in 1992 with their generalization. Popovic showed also that the sequence family has an optimal cross-correlation property. The cross-correlation of generalized Zadoff-Chu sequences was studied in 2012 by Kang et.al. [49] and is currently being studied by many others [50].

We start from the definition of 'correlation' of sequences. We denote by ω a complex primitive p-th root of unity throughout this dissertation. It is easy to find that one of the possible values of ω is $e^{j\frac{2\pi}{p}}$. Note that the complex value $e^{jk\frac{2\pi}{p}}$ for some positive integer k would not be 1 when k is less than p, thus $e^{j\frac{2\pi}{p}}$ is one of the complex primitive p-th root of unities.

Definition 1.2 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. Then the periodic cross-correlation of $\mathbf{u}$ and $\mathbf{v}$ is defined as

$$C(\mathbf{u}, \mathbf{v}, \tau) = \sum_{t=0}^{N-1} \omega^{u(t+\tau)-v(t)}, \quad \tau = 0, 1, 2, \ldots. \tag{1.3}$$

□

Definition 1.3 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 length N. Then the aperiodic cross-correlation of $\mathbf{u}$ and $\mathbf{v}$ is defined as

$$C_A(\mathbf{u}, \mathbf{v}, \tau) = \sum_{t=0}^{N-1-\tau} \omega^{u(t+\tau)-v(t)}, \quad \tau = 0, 1, 2, \ldots. \tag{1.4}$$

□

It is called the periodic autocorrelation when $\mathbf{u} = \mathbf{v}$ or they are cyclically equivalent, and is denoted by $C_{(A)}(\mathbf{u}, \tau)$. 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 $\tau \not\equiv 0 \pmod{N}$.

Example 1.2 A binary sequence of period 4 given by

$$\mathbf{u} = (0, 0, 0, 1, \ldots)$$

is a perfect sequence. Note that a 2-th root of unity is -1, and for each $\tau = 1, 2, 3$,

$$C(\mathbf{u}, 1) = \sum_{t=0}^{N-1} (-1)^{u(t+1)-u(t)} = (-1)^0 + (-1)^0 + (-1)^1 + (-1)^1 = 0,$$

$$C(\mathbf{u}, 2) = \sum_{t=0}^{N-1} (-1)^{u(t+2)-u(t)} = (-1)^0 + (-1)^1 + (-1)^0 + (-1)^1 = 0,$$

$$C(\mathbf{u}, 3) = \sum_{t=0}^{N-1} (-1)^{u(t+3)-u(t)} = (-1)^1 + (-1)^0 + (-1)^0 + (-1)^1 = 0.$$

□

A pair of cyclically distinct perfect sequences is said to be 'optimal' if the magnitude of their periodic cross-correlation is upper bounded by $\sqrt{N}$ [13, 51], and we call such a pair an optimal pair. A sequence family $\mathcal{F}$ is said to be 'optimal' if all the members of $\mathcal{F}$ are perfect and all the pairs from $\mathcal{F}$ are optimal.

An optimal family is said to be 'completely optimal' if the magnitude of cross-correlation of any two members of the family is exactly $\sqrt{N}$.

Example 1.3 Two 3-ary sequences of period 9 given by

$$\mathbf{u} = (0, 1, 2, 1, 0, 2, 2, 2, 2, \ldots)$$

$$\mathbf{v} = (2, 1, 1, 1, 2, 1, 0, 0, 1, \ldots)$$

are perfect sequences and optimal pair with the magnitude of cross-correlation is 3. That is, the sequence family

$$\mathcal{F} = \{\mathbf{u}, \mathbf{v}\}$$

is completely optimal. □

Note that 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 (1.3) is zero for all non-trivial phase shifts. See [17, 52] 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.

Nonbinary integer sequences are also used to represent the slot of signal parameter, like the center frequency. In this case, the concept of Hamming correlation [38] of the nonbinary sequence is studied, for analyze the collision of slots. we start from the definition.

Definition 1.4 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. Then the Hamming periodic cross-correlation of $\mathbf{u}$ and $\mathbf{v}$ of period p, when they are cyclically distinct, is defined as

$$H(\mathbf{u}, \mathbf{v}, \tau) = \sum_{t=0}^{N-1-\tau} h(u(t+\tau), v(t)), \quad \tau = 0, 1, 2, \ldots, \tag{1.5}$$

where $h(x, y) = 1$ if $x = y$ and $h(x, y) = 0$ otherwise. □

Definition 1.5 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 length N. Then the Hamming aperiodic cross-correlation of $\mathbf{u}$ and $\mathbf{v}$ of period p, when they are cyclically distinct, is defined as

$$H_A(\mathbf{u}, \mathbf{v}, \tau) = \sum_{t=0}^{N-1} h(u(t+\tau), v(t)), \quad \tau = 0, 1, 2, \ldots, \tag{1.6}$$

where $h(x, y)$ is same with the Definition 1.4. □

Similarly to the periodic autocorrelation, it is called the Hamming autocorrelation when $\mathbf{u} = \mathbf{v}$ or they are cyclically equivalent, and is denoted by $H_{(A)}(\mathbf{u}, \tau)$. We can easily find that if its non-trivial Hamming periodic autocorrelation is zero, then all the symbols of the sequences must be distinct, that is, $p \geq N$. A pair of cyclically distinct sequences with this property is said to be 'ideal' if the magnitude of their Hamming cross-correlation is upper-bounded by 1. Sequence families with this property is essentially used for design of optimal families in this dissertation.

1.2 Overview

In this dissertation, we will prove 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 property. It is interesting to extend the construction for the Frank-Zadoff sequence, both of which are perfect p-ary polyphase sequences of period p^2. 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 [2] and generates much more different families with the same parameters.

After that, we will derive the conditions for optimal family and general approach to find optimal families including those from Fermat-quotient or Frank-Zadoff sequences. To do this, we introduce a sequence of p-difference, named as 'generator'. After defining the associated family of certain generators, we derive the condition on the generators so that all the sequences in the associated family of the generator are perfect. Moreover, we derive the condition on the generators so that one can form completely optimal families of size $p-1$ by selecting members from certain associated families of the generators. We found some sufficient condition for such generator (we call it an optimal generator) to be used in this way in terms of their Hamming correlation property. We propose an algebraic construction of such generators. The families enclose both the families from Fermat-quotient and Frank-Zadoff sequences, and we indicate their relation also. This section ends with answers to two interesting questions, one of which is the following: Would it be possible to transform the Frank-Zadoff sequence into the Fermat-quotient sequence, or vice versa? If so, then describe the transformation.

After that, we confirm that the construction in this paper covers the families from

optimal generators exhaustively by computers for $p \leq 13$. We conclude this dissertation with some unsolved conjectures, including some relation with Mow's conjecture [17,18] about the number of perfect polyphase sequences.

Chapter 2

Perfectness of the Fermat-quotient Sequences

2.1 The p-ary Fermat-quotient Sequence of period p^2 and its Properties

In this section, we will describe the perfectness and optimality property of the Fermat-quotient sequences defined at Definition 1.1. We will present our first main theorem, which is in fact a corollary to both Theorems 2.2 and 2.3. Since Theorem 2.1 shows special cases of both, we can omit the proof.

Theorem 2.1 Let p be an odd prime. 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

$$\mathcal{F}(\mathbf{q}) = \{m \cdot \mathbf{q} | m = 1, 2, \ldots, p-1\} \tag{2.1}$$

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 $\mathbf{q}$. □

2.1.1 Difference Sequences and RC-Balancedness

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

Definition 2.1 Let p be an odd prime and τ be an integer with $1 \leq \tau < p^2$. 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 $\mathbf{d}_{\mathbf{s},\tau}$ of a p-ary sequence $\mathbf{s}$ of period p^2 as a $p \times p$ array as follows:

$$\mathbf{d}_{\mathbf{s},\tau} = \begin{bmatrix} d_{\mathbf{s},\tau}(0) & d_{\mathbf{s},\tau}(1) & \cdots & d_{\mathbf{s},\tau}(p-1) \\ d_{\mathbf{s},\tau}(p) & d_{\mathbf{s},\tau}(p+1) & \cdots & d_{\mathbf{s},\tau}(2p-1) \\ \vdots & \vdots & \ddots & \vdots \\ d_{\mathbf{s},\tau}((p-1)p) & d_{\mathbf{s},\tau}((p-1)p+1) & \cdots & d_{\mathbf{s},\tau}(p^2-1) \end{bmatrix}. \tag{2.2}$$

We observe that the sequence $\mathbf{s}$ is perfect if its difference sequence $\mathbf{d}_{\mathbf{s},\tau}$ is balanced for all $\tau = 1, 2, \ldots, p^2 - 1$. Note that the autocorrelation of $\mathbf{s}$ defined at Definition 1.2 can be calculated as the sum of powers of the p-th root of unity, where the powers are same with elements of the difference sequence of each τ. And obviously,

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

So, if a p-ary sequence $\mathbf{d}$ of period N is balanced, then

$$\sum_{i=0}^{N-1} \omega^{d(i)} = 0.$$

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 2.2 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 its $p \times p$ array representation of $\mathbf{d}_{\mathbf{s},\tau}$ as shown in (2.2), 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 2.1 is essentially a corollary of the following:

Theorem 2.2 The Fermat-quotient sequence has RC-balanced difference sequences.

Proof: Let $\mathbf{q}$ be the Fermat-quotient sequence.

Case 1 ($\tau = kp \equiv 0 \pmod{p}$): The set of elements from i-th row of (2.2) is given as

$$\begin{aligned}
& \{d_{\mathbf{q},\tau}(pi + j) | j = 0, 1, \ldots, p-1\} \\
= \; & \{q(pi + j + kp) - q(pi + j) | j = 0, 1, \ldots, p-1\} \\
= \; & \{0\} \cup \{-\frac{k}{j} | j = 1, 2, \ldots, p-1\} \qquad (\text{Thethird item of Lemma 1.1}) \\
= \; & \{0, 1, \ldots, p-1\} \qquad \text{since } k \not\equiv 0 \pmod{p}
\end{aligned}$$

Case 2 ($\tau \not\equiv 0 \pmod p$): The set of elements from j-th column of (2.2) is given as

$$\begin{aligned} & \{d_{\mathbf{q},\tau}(pi+j) | i = 0, 1, \ldots, p-1\} \\ = \; & \{q(pi+j+\tau) - q(pi+j) | i = 0, 1, \ldots, p-1\} \end{aligned}$$

Assume that $j \not\equiv 0, -\tau \pmod p$. Then, the third item of Lemma 1.1 implies that the above becomes

$$\begin{aligned} & \{q(j+\tau) - q(j) + i(\frac{1}{j} - \frac{1}{j+\tau}) | i = 1, 2, \ldots, p-1\} \\ = \; & \{0, 1, \ldots, p-1\} \qquad \text{since } \tau \not\equiv 0 \pmod p \end{aligned}$$

Cases with $i \equiv 0, -\tau \pmod p$ can be proved similarly. ■

2.1.2 Transformations of Sequences Preserving RC-Balancedness

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 [9, 26]. Here, we will consider preserving RC-balanced differences. Preserving the RC-balanced differences implies preserving the perfectness, but not conversely in general. Note that the RC-balancedness is just a sufficient condition of the perfectness of the sequence.

Lemma 2.1 Let p be an odd prime and $\mathbf{s} = \{s(t) | t \in \mathbb{Z}\}$ 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 $0 \leq j < p$, $\mathcal{A}_j(\mathbf{s})$ 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.

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 $\tau' \not\equiv 0 \pmod{p}$.

If $\tau \not\equiv 0 \pmod{p}$, $\tau \not\equiv a-b \pmod{p}$, and $\tau \not\equiv b-a \pmod{p}$), then the a-th column of $\mathbf{d}_{\mathbf{s}',\tau}$ is same with the b-th column of $\mathbf{d}_{\mathbf{s},b-a+\tau}$, the $(a-\tau)$-th column of $\mathbf{d}_{\mathbf{s}',\tau}$ is same with the $(a-\tau)$-th column of $\mathbf{d}_{\mathbf{s},b-a+\tau}$, the b-th column of $\mathbf{d}_{\mathbf{s}',\tau}$ is same with the a-th column of $\mathbf{d}_{\mathbf{s},a-b+\tau}$, the $(b-\tau)$-th column of $\mathbf{d}_{\mathbf{s}',\tau}$ is same with the $(b-\tau)$-th column of $\mathbf{d}_{\mathbf{s},a-b+\tau}$, and any other columns of $\mathbf{d}_{\mathbf{s}',\tau}$ are same with the $\mathbf{d}_{\mathbf{s},\tau}$. So the balancedness of columns is preserved.

If $\tau \not\equiv 0 \pmod{p}$ and $\tau \equiv b-a \pmod{p}$), then $a-b \not\equiv \tau \pmod{p}$ since p is a prime. The a-th column of $\mathbf{d}_{\mathbf{s}',\tau}$ is same with the a-th column of $\mathbf{d}_{\mathbf{s},\tau}$ multiplied by -1, the $(a-\tau)$-th column of $\mathbf{d}_{\mathbf{s}',\tau}$ is same with the $a-\tau$-th column of $\mathbf{d}_{\mathbf{s},2\tau}$, the b-th column of $\mathbf{d}_{\mathbf{s}',\tau}$ is same with the a-th column of $\mathbf{d}_{\mathbf{s},2\tau}$, and any other columns of $\mathbf{d}_{\mathbf{s}',\tau}$ are same with the $\mathbf{d}_{\mathbf{s},\tau}$. So the balancedness of columns is preserved. The case with $a-b \equiv \tau \pmod{p}$ is proved by the same way.

Therefore, column-balancedness is preserved. ■

Example 2.1 We consider the case $p = 5$ in Table 2.1. Here, $\mathbf{q}$ is the Fermat-quotient sequence. Observe that all the transforms are not only perfect, but also have RC-balanced differences. □

Table 2.1: The Fermat-quotient sequence and its transforms for $p = 5$. Here, $\sigma = (043)$ in cycle notation.

$\mathbf{s}$	Array of $\mathbf{s}$	$\mathbf{d}_{\mathbf{s},1}$ (column balanced)	$\mathbf{d}_{\mathbf{s},5}$ (row balanced)
$\mathbf{q}$	$\begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 3 & 3 & 0 & 4 \\ 4 & 1 & 4 & 3 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 2 & 1 & 4 & 1 \\ 1 & 0 & 2 & 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \end{bmatrix}$
$2 \cdot \mathbf{q}$	$\begin{bmatrix} 0 & 0 & 1 & 2 & 2 \\ 0 & 3 & 0 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \\ 0 & 4 & 3 & 0 & 3 \\ 0 & 2 & 2 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 1 & 0 & 3 \\ 3 & 2 & 3 & 1 & 1 \\ 1 & 3 & 0 & 2 & 4 \\ 4 & 4 & 2 & 3 & 2 \\ 2 & 5 & 4 & 4 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 3 & 4 & 1 & 2 \\ 0 & 3 & 4 & 1 & 2 \\ 0 & 3 & 4 & 1 & 2 \\ 0 & 3 & 4 & 1 & 2 \\ 0 & 3 & 4 & 1 & 2 \end{bmatrix}$
$\mathcal{A}_3(\mathbf{q})$	$\begin{bmatrix} 0 & 0 & 3 & 2 & 1 \\ 0 & 4 & 0 & 0 & 2 \\ 0 & 3 & 2 & 3 & 3 \\ 0 & 2 & 4 & 1 & 4 \\ 0 & 1 & 1 & 4 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 3 & 4 & 4 & 4 \\ 4 & 1 & 0 & 2 & 3 \\ 3 & 4 & 1 & 0 & 2 \\ 2 & 2 & 2 & 3 & 1 \\ 1 & 0 & 3 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \end{bmatrix}$
$\mathcal{P}_\sigma(\mathbf{q})$	$\begin{bmatrix} 1 & 0 & 3 & 1 & 0 \\ 4 & 4 & 0 & 2 & 0 \\ 2 & 3 & 2 & 3 & 0 \\ 0 & 2 & 4 & 4 & 0 \\ 3 & 1 & 1 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 3 & 3 & 4 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 4 & 1 & 2 & 2 \\ 2 & 2 & 0 & 1 & 0 \\ 3 & 0 & 4 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 3 & 4 & 2 & 1 & 0 \\ 3 & 4 & 2 & 1 & 0 \\ 3 & 4 & 2 & 1 & 0 \\ 3 & 4 & 2 & 1 & 0 \\ 3 & 4 & 2 & 1 & 0 \end{bmatrix}$

2.2 Generalized Optimal Families from Fermat-quotient Sequences

We would like to recall that the family in Theorem 2.1 is obtained by applying all possible constant multiplications (First item of Lemma 2.1). Now, we consider the second transformation of Lemma 2.1. We denote:

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

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:

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

The following theorem gives a generalized version of the family in Theorem 2.1 including the Constant Column Additions as well as the Constant Multiples. That is, the second item of Theorem 2.1 is a corollary to the following:

Theorem 2.3 (main of Chapter 2) Let p be an odd prime and $\mathbf{a}_m$ 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

$$\mathcal{F}_A(\mathbf{q}) = \{m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{q}) | m = 1, 2, ..., p-1\}. \tag{2.3}$$

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

Proof: For any $m \not\equiv 0 \pmod p$ and any integer sequence $\mathbf{a}_m$ of period p, the p-ary sequence $m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{q})$ is perfect by Theorem 2.2 and Lemma 2.1.

Now, we derive the cross-correlation of a pair from $\mathcal{F}_A(\mathbf{q})$. Assume that $m \not\equiv n \pmod p$ and $m, n \not\equiv 0 \pmod p$, and $\mathbf{a}$ and $\mathbf{b}$ are any arbitrary integer sequences of period p not necessarily distinct. Then,

$$\begin{aligned} C(m \cdot \mathcal{A}^{\mathbf{a}}(\mathbf{q}), n \cdot \mathcal{A}^{\mathbf{b}}(\mathbf{q}), \tau) &= \sum_{t=0}^{p^2-1} \omega^{m(q(t+\tau)+a(t+\tau)) - n(q(t)+b(t))} \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{mq(pi+j+\tau) - nq(pi+j) + ma(j+\tau) - nb(j)} \qquad (\text{where } t \triangleq pi + j) \\ &\triangleq A + B, \end{aligned}$$

where

$$A \triangleq \sum_{i=0}^{p-1} \omega^{mq(pi+\tau)-nq(pi)+ma(\tau)-nb(0)}$$
$$= \omega^{ma(\tau)-nb(0)} \sum_{i=0}^{p-1} \omega^{mq(pi+\tau)-nq(pi)}$$

is the sum for $j = 0$, and

$$B \triangleq \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} \omega^{mq(pi+j+\tau)-nq(pi+j)+ma(j+\tau)-nb(j)}$$
$$= \sum_{j=1}^{p-1} \omega^{ma(j+\tau)-nb(j)} \sum_{i=0}^{p-1} \omega^{mq(pi+j+\tau)-nq(pi+j)}$$

is the sum of remaining terms for $j \neq 0$.

Recall that $q(pi) = 0$ for all i, and $q(pi+j)$ for $j \not\equiv 0 \pmod{p}$ runs from 0 to $p-1$ in some order as i runs from 0 to $p-1$. Therefore,

$$A = \begin{cases} p\omega^{ma(0)-nb(0)} & \text{if } \tau \equiv 0 \pmod{p} \\ 0 & \text{otherwise} \end{cases}.$$

The inner sum B' of B becomes the following:

$$B' \triangleq \sum_{i=0}^{p-1} \omega^{mq(pi+j+\tau)-nq(pi+j)}$$

Case 1: When $\tau \equiv 0 \pmod{p}$, or $\tau = kp$ for some k,

$$B' = \sum_{i=0}^{p-1} \omega^{mq(p(i+k)+j)-nq(pi+j)}$$
$$= \sum_{i=0}^{p-1} \omega^{m\left(q(j)-\frac{i+k}{j}\right)-n\left(q(j)-\frac{i}{j}\right)}$$
$$= \omega^{(m-n)q(j)-m\frac{k}{j}} \sum_{i=0}^{p-1} \omega^{i\frac{n-m}{j}}$$
$$= 0 \qquad \text{since } m \not\equiv n \pmod{p} \text{ and } j \not\equiv 0 \pmod{p}.$$

Case 2: When $\tau \not\equiv 0 \pmod{p}$, we distinguish the cases $j+\tau \equiv 0$ and $j+\tau \not\equiv 0$.

For $j+\tau \equiv 0 \pmod{p}$,

$$\begin{aligned} B' &= \sum_{i=0}^{p-1} \omega^{mq(pi)-nq(pi-\tau)} \\ &= \sum_{i=0}^{p-1} \omega^{-nq(pi-\tau)} = 0, \end{aligned}$$

since $\tau \not\equiv 0 \pmod{p}$ and $(-\tau)$-th column of $\mathbf{q}$ is balanced. For $j+\tau \not\equiv 0 \pmod{p}$,

$$\begin{aligned} B' &= \sum_{i=0}^{p-1} \omega^{m\left(q(j+\tau)-\frac{i}{j+\tau}\right)-n\left(q(j)-\frac{i}{j}\right)} \\ &= \omega^{mq(j+\tau)-nq(j)} \sum_{i=0}^{p-1} \omega^{i\left(\frac{n}{j}-\frac{m}{j+\tau}\right)}. \quad = \begin{cases} p\omega^{mq(j+\tau)-nq(j)} & \text{if } \frac{n}{j}-\frac{m}{j+\tau} \equiv 0 \pmod{p} \\ 0 & \text{otherwise} \end{cases}. \end{aligned}$$

Therefore, when $\tau \not\equiv 0 \pmod{p}$, letting $j_0 = \frac{n\tau}{m-n}$,

$$\begin{aligned} B &= \omega^{ma(j_0+\tau)-nb(j_0)} \cdot B' \\ &= p\omega^{m(q(j_0+\tau)+a(j_0+\tau))-n(q(j_0)+b(j_0))}. \end{aligned}$$

■

Example 2.2 Table 2.2 shows optimal families from Theorems 2.1 and 2.3 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 $\mathbf{a}_1 = (0,0,0,0,0), \mathbf{a}_2 = (0,0,1,0,0), \mathbf{a}_3 = (2,0,0,0,1), \mathbf{a}_4 = (0,1,2,3,4)$. □

Remark 2.1 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 2.3 works even if the integer sequences $\mathbf{a}_m$ are all the same. We have checked the

Table 2.2: Example of optimal families from the Fermat-quotient sequence for $p = 5$.

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

other direction by computer for $p \leq 7$: 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. □

2.3 Relations with Frank-Zadoff Sequences

It is well-known in [9, 10] 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 dissertation.

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 (1.2). Such a $p \times p$ array of $\mathbf{z}$ is the result of modulo p reduction of the following:

$$\begin{bmatrix} 1 & 2 & 3 & \cdots & p \\ 2 & 4 & 6 & \cdots & 2p \\ 3 & 6 & 9 & \cdots & 3p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p & 2p & 3p & \cdots & p^2 \end{bmatrix} \tag{2.4}$$

We note that Theorem 2.1 will work if the sequence is replaced with the Frank-Zadoff sequence, which is the well-known results from many others [2, 9, 10].

Similar to the last item of Lemma 1.1, for the p-ary Frank-Zadoff sequence $\mathbf{z} = \{z(t)|t \in \mathbb{Z}\}$ of period p^2, we have

$$z(t + kp) \equiv z(t) + k(t + 1) \pmod{p}, \tag{2.5}$$

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 (2.4), that all the columns and rows are balanced except for the right-most column and the bottom row.

It turned out that Theorem 2.2 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 will not be too much surprising that Theorem 2.3 will also work 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.

Chapter 3

Optimal Families of Perfect Polyphase Sequences

3.1 Optimal Generators

Recall that we construct optimal families of the form $m \cdot \mathbf{s}$ in Theorem 2.1 and of the form $m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{s})$ in Theorem 2.3, 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 2.1. We hope that, when $\mathbf{s}$ is a p-ary perfect sequence of period p^2, some set of sequences given by

$$\mathcal{F}_P(\mathbf{s}) = \{m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathcal{P}_\sigma(\mathbf{s}))|m = 1, 2, \ldots, p-1\} \tag{3.1}$$

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. We hope that in this way we find the Frank-Zadoff sequence in $\mathcal{F}_P(\mathbf{s})$ when we substitute $\mathbf{s}$ for the Fermat-quotient sequence in (3.1), or vice versa. We will eventually answer to all these questions in this section.

It turned out that not every σ results in an optimal family in (3.1) even for the Fermat-

quotient sequence or the Frank-Zadoff sequence. It is obvious that the following two cases work and in fact it is implicitly mentioned in [26]:

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. For the Fermat-quotient and Frank-Zadoff sequence, the column-rotation can be represented as a constant column addition transformation, since both sequences have constant difference in every column (See (2.5) and the third item of Lemma 1.1). In general, if a sequence with RC-balanced difference sequences has constant difference in every column, the column rotation becomes equivalent with the constant column addition.

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 $d_{\mathbf{s},p}(0), d_{\mathbf{s},p}(1), \ldots, d_{\mathbf{s},p}(p-1)$.

3.1.1 Generators and Optimal Families

Definition 3.1 Let p be an odd prime. 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 sequences having $\mathbf{g}$ as their common generator is the associated family of $\mathbf{g}$, denoted by $\mathcal{S}(\mathbf{g})$. □

Remark 3.1 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 $j = 0, 1, ..., p-1$,

$$s(pi + j) = g(j)i + s(j). \tag{3.2}$$

That is,

$$\begin{aligned}
\mathbf{s} &= \begin{bmatrix} s(0) & s(1) & \cdots & s(p-1) \\ s(0)+g(0) & s(1)+g(1) & \cdots & s(p-1)+g(p-1) \\ s(0)+2g(0) & s(1)+2g(1) & \cdots & s(p-1)+2g(p-1) \\ \vdots & \vdots & \ddots & \vdots \\ s(0)+(p-1)g(0) & s(1)+(p-1)g(1) & \cdots & s(p-1)+(p-1)g(p-1) \end{bmatrix} \\
&= \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} [s(0) \;\; s(1) \;\; \cdots \;\; s(p-1)] + \begin{bmatrix} 0 \\ 1 \\ \vdots \\ p-1 \end{bmatrix} [g(0) \;\; g(1) \;\; \cdots \;\; g(p-1)] \\
&\triangleq \underline{\mathbf{1}}^T \underline{\mathbf{s}} + \underline{\delta}^T \underline{\mathbf{g}},
\end{aligned} \tag{3.3}$$

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 3.2 From the third property of Fermat-quotient sequences in *Lemma 1.1* and (3.2), it is obvious that Fermat-quotient sequences have a generator given as

$$g(j) \equiv -j^{p-2} \pmod{p} \tag{3.4}$$

for all $j \in \mathbb{Z}_p$. Similarly, from (2.5) and (3.2), it is obvious that Frank-Zadoff sequences have a generator given as

$$g(j) \equiv j + 1 \pmod{p} \tag{3.5}$$

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 3.1 Let p be an odd prime and 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 3.1 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:

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

□

Remark 3.3 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 3.3, 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 3.2 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 3.2, an optimal generator is a perfect generator, but not conversely. Example 3.2 shows a perfect generator that is not an optimal generator.

Example 3.2 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 3.4 that the generators of the Fermat-quotient sequences and the Frank-Zadoff sequences are optimal generators. □

Theorem 3.1 (main of Chapter 3) Let p be an odd prime and $\mathbf{g}$ be an optimal generator of period p. Then, picking up any one member $\mathbf{s}_m$ from $\mathcal{S}(m \cdot \mathbf{g})$ for each $m = 1, 2, \ldots, p-1$ gives an optimal family

$$\mathcal{F}_G(\mathbf{g}) = \{\mathbf{s}_m | m = 1, 2, \ldots, p-1\} \tag{3.6}$$

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 the optimal generators. Note that the number of members in a family $\mathcal{F}_G(\mathbf{g})$ is $p-1$. 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 (3.1). 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 (3.1). Therefore, in order to characterize those permutations σ, we only have to characterize optimal generators.

3.1.2 Perfect Generators

The following lemma is about the vector sum of a prime regular polygon used in the proof of Theorem 3.2. Its proof is implied by last part of proof of Theorem 1 of [18].

Lemma 3.2 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

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

□

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, we note that a generator $\mathbf{g}$ is balanced if its one period is a permutation of $\{0, 1, 2, \ldots, p-1\}$.

Theorem 3.2 (Perfect Generator Construction) Let p be an odd prime. The followings are equivalent:

1. $\mathbf{g}$ is a perfect generator.

2. $\mathbf{g}$ is balanced, or equivalently, it is a permutation of $\{0, 1, 2, \ldots, p-1\}$.

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 (3.3).

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 3.2, 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 ($\tau = kp \equiv 0 \pmod{p}$): The set of elements from i-th row of the array representation of $d_{\mathbf{s},kp}$ is given as

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

   which must be balanced since $k \not\equiv 0 \pmod{p}$ and $g(j)$ is balanced.

   Case 2 ($\tau \not\equiv 0 \pmod{p}$): The set of elements from j-th column of the array representation of $d_{\mathbf{s},\tau}$ is given as

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

   which must be balanced since $g(j+\tau) \not\equiv g(j) \pmod{p}$ for any j.

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

Remark 3.4 Note that the result of the construction in Theorem 3.2 does not produce new perfect sequences. All the sequences in the associated family of the perfect generators from Theorem 3.2 are essentially the same as those obtained by Heimiller's generalization [10]. The sequences are also considered in [16] as bent functions, and are treated at Mow's unified construction [17, 52]. □

3.1.3 Optimal Generators

We determine the property of optimal generators. To do this, we have to use the definition of periodic Hamming cross-correlation defined at Definition 1.4. Note that $H(\mathbf{u}, \mathbf{v}, \tau) = 1$ is equivalent to having a unique solution of t to $u(t+\tau) \equiv v(t) \pmod{p}$.

Theorem 3.3 Let p be an odd prime. A generator $\mathbf{g}$ of period p 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 3.1 from $\mathbf{g}$ 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 $0 \leq a < p$ and $1 \leq b < p$. Observe that $g(a) \not\equiv 0 \pmod{p}$, since otherwise, $H \geq 2$ for all $m \neq n$ for $\tau = b$. Note that $H(m \cdot \mathbf{g}, n \cdot \mathbf{g}, \tau) = 1$ for any τ and any $m \neq n$ implies that there exists a unique solution t in $0 \leq t < p$ to the equation $mg(t+\tau) \equiv ng(t) \pmod{p}$ for

any given $m \neq n$ and τ. Note also that there exists a unique z in $0 \leq z < p$ 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 $H(m \cdot \mathbf{g}, \mathbf{g}, \tau = b) \geq 2$. Similarly, we have $t_m \not\equiv z - b \pmod{p}$ and $t_m \not\equiv a \pmod{p}$. Since the three elements z, $z - b$, a must all be distinct mod p, we have

$$|\{t_m | m = 2, 3, ..., p - 1\}| \leq p - 3. \tag{3.7}$$

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 (3.7). Therefore $\mathbf{g}$ must contain any symbol at most once. Since it has period p, it must be balanced.

(Proof of optimality) From Lemma 2.1, $m \cdot \mathbf{g}$ 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 exists 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,

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

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

$$\begin{aligned} C(\mathbf{u}, \mathbf{v}, \tau) &= C(m \cdot \mathcal{A}^{\mathbf{a}}(\mathbf{s}), n \cdot \mathcal{A}^{\mathbf{b}}(\mathbf{s}), \tau) \\ &= \sum_{t=0}^{p^2-1} \omega^{ms(t+\tau)-ns(t)+ma(t+\tau)-nb(t)} \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{ms(pi+j+\tau)-ns(pi+j)+ma(pi+j+\tau)-nb(pi+j)} \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \omega^{ms(j+\tau)+mig(j+\tau)-ns(j)-nig(j)+ma(j+\tau)-nb(j)} \\ &= \sum_{j=0}^{p-1} \omega^{ms(j+\tau)-ns(j)+ma(j+\tau)-nb(j)} \sum_{i=0}^{p-1} \omega^{i\{mg(j+\tau)-ng(j)\}} \end{aligned} \tag{3.8}$$

Now, the inner sum of (3.8) 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 3.5 Theorem 3.3 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 3.3 for $p \leq 13$ using computers. □

Theorem 3.4 gives some transformations that preserve the optimality of a generator.

Theorem 3.4 Let p be an odd prime. 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 (3.3), we have

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

   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 $d \not\equiv 0 \pmod{p}$ [26]. 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 3.4 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 3.4:

Definition 3.3 Let p be an odd prime. 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 3.4. □

Example 3.3 We can find an optimal generator $\mathbf{g} = (0, 1, 2, 3, 4)$ at $p = 5$. Then, its cyclic shifts

$$(1, 2, 3, 4, 0), (2, 3, 4, 0, 1), (3, 4, 0, 1, 2), (4, 0, 1, 2, 3),$$

its constant multiples

$$(0, 2, 4, 1, 3), (0, 3, 1, 4, 2), (0, 4, 3, 2, 1),$$

and combinations of two operations

$$(2,4,1,3,0),(1,4,2,0,3),(2,1,0,4,3),\cdots$$

are also optimal generators, and all of them are equivalent with $\mathbf{g}$. □

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 3.3. We denote by $\mathrm{Class}(\mathbf{g})$ the equivalence class containing the generator $\mathbf{g}$.

Lemma 3.3 Let p be an odd prime and 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 $\mathbf{h} \in \mathrm{Class}(\mathbf{g})$ such that $h(0) = 0$ and $h(1) = 1$.
2. These are equivalent:
   (a) There exists $\mathbf{h} \in \mathrm{Class}(\mathbf{g})$ 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 $\mathrm{Class}(\mathbf{g})$.
   (c) Any decimation of $\mathbf{g}'$ belongs to $\mathrm{Class}(\mathbf{g})$ for any $\mathbf{g}' \in \mathrm{Class}(\mathbf{g})$.

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 $\mathbf{h} \in \mathrm{Class}(\mathbf{g})$. 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 $\mathcal{D}_d(\mathbf{g}) \in \mathrm{Class}(\mathbf{h}) = \mathrm{Class}(\mathbf{g})$ 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 $\mathrm{Class}(\mathbf{g}') = \mathrm{Class}(\mathbf{g})$.

   (c) $\rightarrow$ (a): From Lemma 3.3-1), we can find $\mathbf{h}$ that any decimation of $\mathbf{h}$ belongs to $\mathrm{Class}(\mathbf{g})$ 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 3.5 Let $\mathbf{g}$ be a balanced p-ary generator of period p. If $\mathbf{g}$ is equivalent in the sense of Definition 3.3 with all its decimations, then it satisfies the Hamming correlation property in Theorem 3.3. Hence, it is an optimal generator.

Proof: Assume that all the decimations of $\mathbf{g}$ are equivalent with $\mathbf{g}$. From the second item of Lemma 3.3, this implies the existence of a generator $\mathbf{h} \in \mathrm{Class}(\mathbf{g})$ 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 3.3. Then, $\mathbf{h}$ is an optimal generator, and hence, so is $\mathbf{g}$.

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 τ, $m, n \not\equiv 0 \pmod{p}$ 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

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

or

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

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

Remark 3.6 It is open whether the converse of Theorem 3.5 is true in general. We confirmed that this is true for $p \leq 23$ using computers. □

The following lemma gives two optimal generators corresponded by Fermat-quotient and Frank-Zadoff sequences, which we have observed their optimality in Theorem 2.3.

Lemma 3.4 Let p be an odd prime. The generator of Fermat-quotient sequences given by *(Remark 3.2)*

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

is an optimal generator. So is the generator of Frank-Zadoff sequences given by *(Remark 3.2)*

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

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 3.5. 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 3.5. 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 3.3. 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 3.3, we have $g(\alpha^l) = \beta^l$ for any $l = 0, 1, 2, ...$ Since $\mathbf{g}$ is balanced, β must also be a primitive root of p. That is, the

following generator $\mathbf{g}$ with:

$$g(t) = \begin{cases} 0 & t = 0 \\ 1 & t = 1 \\ \beta^{\log_\alpha t} & \text{otherwises} \end{cases}$$

becomes an optimal generator where α and β are primitive roots of p. It directly indicates the following construction.

Theorem 3.6 (Optimal Generator Construction) Let p be an odd prime, 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:

$$g(t; p, \kappa, m, \tau) \equiv m(t + \tau)^\kappa \pmod{p}, \tag{3.9}$$

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 3.3.

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 3.3 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 3.7 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 3.6, 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 3.6. □

Remark 3.8 Observe that, from Lemma 3.4, the integer sequence $\mathbf{g}(p, p-2, p-1, 0)$ is the generator of p-ary Fermat-quotient sequence, and the integer sequence $\mathbf{g_z} = \mathbf{g}(p, 1, 1, 1)$ 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 3.4 also proves Theorems 2.2 and 2.3. Furthermore, note that we obtain an optimal family $\mathcal{F}_G(\mathbf{g})$ in Theorem 3.1 when we use the generator $\mathbf{g}(p, 1, 1, 1)$ of a p-ary Frank-Zadoff sequence. This gives a proof of the assertion at the end of Chapter 2 that Theorem 2.3

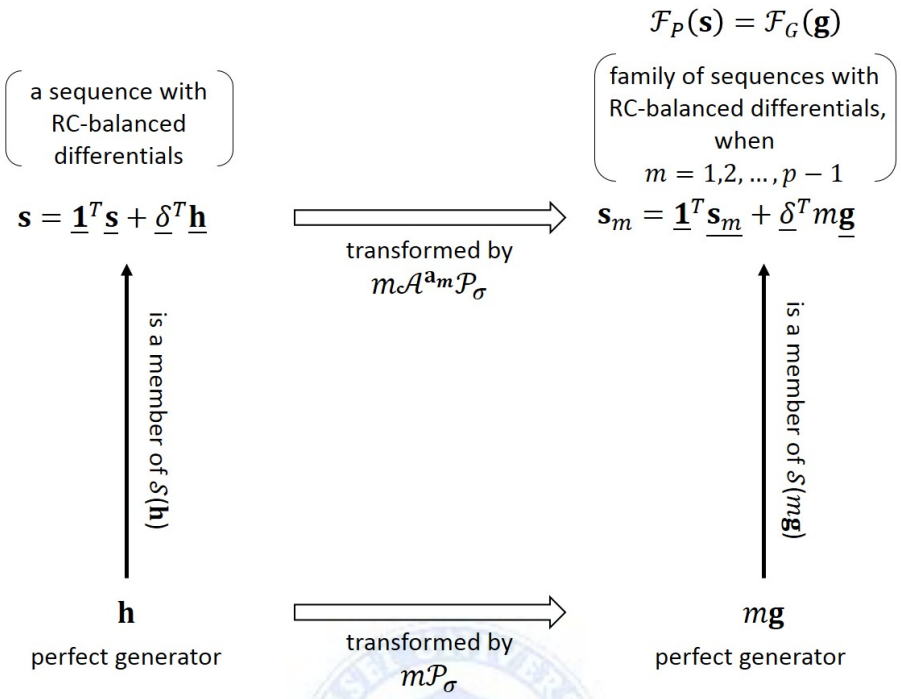

Figure 3.1: Relation of transforms between generators and members of their associated families

will work if the sequence is replaced with the Frank-Zadoff sequence. That is, one can arrange such that

$$\{\mathbf{s}_m \in \mathcal{S}(m \cdot \mathbf{g}_\mathbf{z}) | m = 1, 2, \dots, p-1\} = \{m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{z}) | m = 1, 2, ..., p-1\},$$

where $\mathbf{z}$ is the p-ary Frank-Zadoff sequence of period p^2. Here, for any $m = 1, 2, ..., p-1$, and for any $\mathbf{a}_m$, the sequence $\mathbf{s}_m$ is selected from $\mathcal{S}(m \cdot \mathbf{g}_\mathbf{z})$ whose initial p terms are coincide with those of $m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathbf{z})$. □

Now we get back to the questions raised in the beginning of this section.

- For which column permutations σ is the family given in (3.1) optimal?

- Would it be possible to transform the Frank-Zadoff sequence into the Fermat-quotient sequence, or vice versa? If so, then describe the transformation.

For this, we will explain how a transform (or a permutation σ) of one balanced generator into another leads to the transform between members of their associated families using Fig. 3.1. In this figure, we start from a perfect generator $\mathbf{h}$, and we pick up a member sequence $\mathbf{s}$ from the associated family $\mathcal{S}(\mathbf{h})$. Let $m \in \{1, 2, ..., p-1\}$. The permutation σ on $\mathbf{h}$ can be regarded as a column permutation of $\mathcal{P}_\sigma$ on $1 \times p$ matrix $\underline{\mathbf{h}}$. Thus, $m\mathcal{P}_\sigma$ transforms $\mathbf{h}$ into $m\mathbf{g}$, which must also be a perfect generator. For each m, we pick up a member $\mathbf{s}_m$ from the associated family $\mathcal{S}(m\mathbf{g})$ to form a family of sequences $\{\mathbf{s}_m | m = 1, 2, ..., p-1\}$. On the other hand, the sequence $\mathbf{s}$ can be transformed by $m \cdot \mathcal{A}^{\mathbf{a}_m}(\mathcal{P}_\sigma(\mathbf{s}))$, and obtain a family using $m = 1, 2, ..., p-1$. Now we claim the following and prove it carefully:

Theorem 3.7 Assume the situation in Figure 3.1, and the transformations described just above. Then, for each m, two sequences through both processes coincide with each other when $\mathbf{a}_m$ in one direction and the initial vector $\underline{\mathbf{s}}_m$ in the other direction are suitably selected.

Proof: The representation of $\mathbf{s}_m$ in Fig. 3.1 is from Remark 3.1. Let $\mathbf{s}'_m$ be the result of the transformation $m \cdot \mathcal{A}^{\mathbf{a}_m}\mathcal{P}_\sigma$ of $\mathbf{s}$. Then

$$\begin{aligned}
\mathbf{s}'_m &= m \cdot \mathcal{A}^{\mathbf{a}_m}\mathcal{P}_\sigma(\mathbf{s}) \\
&= m \cdot \mathcal{A}^{\mathbf{a}_m}\mathcal{P}_\sigma(\underline{\mathbf{1}}^T\underline{\mathbf{s}} + \underline{\delta}^T\underline{\mathbf{h}}) \\
&= m \cdot \mathcal{A}^{\mathbf{a}_m}(\underline{\mathbf{1}}^T\mathcal{P}_\sigma(\underline{\mathbf{s}}) + \underline{\delta}^T\mathcal{P}_\sigma(\underline{\mathbf{h}})) \\
&= m \cdot (\underline{\mathbf{1}}^T\mathcal{A}^{\mathbf{a}_m}\mathcal{P}_\sigma(\underline{\mathbf{s}}) + \underline{\delta}^T\mathcal{P}_\sigma(\underline{\mathbf{h}})) \\
&= \underline{\mathbf{1}}^T m \cdot \mathcal{A}^{\mathbf{a}_m}\mathcal{P}_\sigma(\underline{\mathbf{s}}) + \underline{\delta}^T m \cdot \mathcal{P}_\sigma(\underline{\mathbf{h}}) \\
&\stackrel{?}{=} \underline{\mathbf{1}}^T\underline{\mathbf{s}}_m + \underline{\delta}^T m\underline{\mathbf{g}} = \mathbf{s}_m
\end{aligned}$$

Therefore, $\mathbf{s}'_m = \mathbf{s}_m$ if and only if

$$\begin{aligned}
\underline{\mathbf{s}}_m &= m \cdot \mathcal{A}^{\mathbf{a}_m}\mathcal{P}_\sigma(\underline{\mathbf{s}}), \quad \text{and} \\
\underline{\mathbf{g}} &= \mathcal{P}_\sigma(\underline{\mathbf{h}}).
\end{aligned}$$

■

Corollary 3.1 Assume the situation in Figure 3.1, and the transformations described in Theorem 3.7. The transform $\mathcal{P}_\sigma$ results in an optimal generator $\mathbf{g}$ if and only if the transform $\mathcal{A}^{\mathbf{a}_m}\mathcal{P}_\sigma$ results in an optimal family. □

This corollary gives an answer to the first question: a column permutation σ will result in an optimal family of the form (3.1) if and only if it will transform the generator of $\mathbf{s}$ into an optimal generator. For the second question, the final relation we have identified in the proof of Theorem 3.7 gives an answer. Let $\mathbf{h} = \mathbf{g}_z$ be the generator of Frank-Zadoff sequence and use $\mathbf{s} = \mathbf{z}$ which must be a member of $\mathcal{S}(\mathbf{g}_z)$. Then,

one can determine uniquely the permutation σ which transforms $\mathbf{g}_z$ into the generator of Fermat-quotient sequence. Now, the integer sequence $\mathbf{a}_1$ (or an integer vector of length p) can be uniquely determined from the relation

$$\underline{\mathbf{s}}_1 = \mathcal{A}^{\mathbf{a}_1}\mathcal{P}_\sigma(\underline{\mathbf{s}}) = \mathbf{a}_1 + \mathcal{P}_\sigma(\underline{\mathbf{s}}),$$

where $\underline{\mathbf{s}}_1$ denotes the first p terms of Fermat-quotient sequence, $\underline{\mathbf{s}}$ denotes the first p terms of Frank-Zadoff sequence, and σ is the one determined above. That is,

$$\mathbf{a}_1 = \mathcal{P}_\sigma(\underline{\mathbf{s}}) - \underline{\mathbf{s}}_1.$$

Remark 3.9 The $p \times p$ array structure of both Fermat-quotient sequences and Frank-Zadoff sequences gives a clue to how they are related in their equations. From the third property in Lemma 1.1 and (3.5), 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 $j \not\equiv 0 \pmod{p}$,

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

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

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

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

3.2 Counting the Number of Families

To count the number of different families from Theorems 3.1 and 3.6, We start from observing the number of different $\mathbf{g}(p, \kappa, m, y)$ for given p. The number becomes $\varphi(p-1) \cdot (p-1)p$, implied from the number of possible combinations of parameters. However, we observed that the families from $\mathcal{F}_G(\mathbf{g}(p, \kappa, m, \tau))$ and $\mathcal{F}_G(\mathbf{g}(p, \kappa, n, \tau))$ are essentially same even if $m \not\equiv n \pmod{p}$. In other word, we cannot make a family from $\mathcal{F}_G(\mathbf{g}(p, \kappa, m, \tau))$ that cannot be constructed from $\mathcal{F}_G(\mathbf{g}(p, \kappa, n, \tau))$. Thus, there exist $\varphi(p-1)p$ choices of $\mathbf{g}$ for $\mathcal{F}_G(\mathbf{g})$ from Theorem 3.6. Next we will observe the number of different families of $\mathcal{F}_G(\mathbf{g})$ from given $\mathbf{g}$. Note that the size of associated family $\mathcal{S}(\mathbf{g}(p, \kappa, m, \tau))$ is p^p, and selecting member from $\mathcal{S}(\mathbf{g}(p, \kappa, m, \tau))$ can be individually performed at each $m = 1, 2, \ldots, p-1$. Thus, there exist $(p^p)^{(p-1)}$ different families of $\mathcal{F}_G(\mathbf{g})$ for given $\mathbf{g}$. As a result, we can find $\varphi(p-1)p^{p^2-p+1}$ different families from Theorems 3.1 and 3.6.

For the convenience, we say two 'families' are cyclically equivalent if every members in one is cyclically equivalent with some member in another. Otherwise, we say two families are cyclically inequivalent. Note that it is not appropriate to say that two optimal families are different if they are cyclically equivalent. In this reason, we've tried to

analyze the number of cyclically inequivalent families from Theorems 3.1 and 3.6 also. To obtain the number, we start from the number of cyclically inequivalent members of an associated family.

From Lemma 3.1, we can say that there exist $\frac{p^p}{p} = p^{p-1}$ members in an associated family which are cyclically inequivalent with each other. Note that two sequences having generators $\mathbf{g}(p, \kappa, m, \tau)$ and $\mathbf{g}(p, \lambda, n, \mu)$ for each are cyclically inequivalent if $\kappa \not\equiv \lambda \pmod{p-1}$ or $m \not\equiv n \pmod{p}$. However, τ and μ does not work in the same way. The proof of the first item of Theorem 3.4 indicates that two families $\mathcal{S}(\mathbf{g}(p, \kappa, m, \tau))$ and $\mathcal{S}(\mathbf{g}(p, \kappa, m, \mu))$ are cyclically equivalent for any integers τ and μ. Varying κ and selecting each member from cyclically inequivalent members in $\mathcal{S}(\mathbf{g}(p, \kappa, m, \tau))$ for each m, we can find $\varphi(p-1)\left(p^{p-1}\right)^{(p-1)} = \varphi(p-1)p^{(p-1)^2}$ families with all of them are cyclically inequivalent with each other.

Observe that there are a lot of cyclically inequivalent families sharing a same sequence as their member. More specifically, it is easy to show that there are $p^{(p-1)(p-1-k)}$ cyclically inequivalent families sharing k same sequences $(1 \leq k \leq p-1)$. In this case we regard that two cyclically equivalent sequences is same sequence. The number is a bit ambiguous to explain the number of family, therefore, our final observation in this section is to find the number of families that all the families do not share a same member with each other. For the convenience, we say that two families are 'completely distinct' if any member in a family cannot be obtained from the cyclic shift of any member in another, that is, they do not share a same member with each other.

It is easy to show that $\mathcal{F}_G(\mathbf{g}(p, \kappa, 1, 0))$ and $\mathcal{F}_G(\mathbf{g}(p, \lambda, 1, 0))$ with $\kappa \not\equiv \lambda \pmod{p-1}$ are not only cyclically inequivalent, but also completely distinct. We count the num-

ber by progressive method using this fact. At first, we select κ from $\varphi(p-1)$ candidates. Next we choose the first family. There exist p^p possible choices of members for each associated families. After choosing the first, we choose the second family. There exist $p^p - p$ possible choices for each associated families to make all of them are cyclically inequivalent with the first. In the same way, there exist $p^p - 2p$ possible choices for each associated families choosing the third family. In general, there exist $p^p - (k-1)p$ possible choices for each associated families choosing the k-th family. After choosing p^{p-1} families in this way, the possible choices are extinguished. So we can say that we can find p^{p-1} completely distinct families with given κ. Varying κ, we can find $\varphi(p-1)p^{p-1}$ families with all of them are completely distinct with each other.

Theorem 3.8 Let p be an odd integer. There exist $\varphi(p-1)p^{(p-1)^2}$ cyclically inequivalent optimal families of p-ary sequences with period p^2 and family size $p-1$ from Theorems 3.1 and 3.6. Moreover, there exist at least $\varphi(p-1)p^{p-1}$ completely distinct optimal families of p-ary sequences with period p^2 and family size $p-1$ from Theorems 3.1 and 3.6. □

Observe that Theorem 3.1 with Theorem 3.6 gives far larger variation of families than the construction of Popovic [12], that is used in 3GPP LTE, while Popovic gives p completely distinct optimal families of family size $p-1$. Mow's method [52], that had been give the largest variation of families ever known, gives p^{p-1} completely distinct optimal families of family size $p-1$. That is, our method gives the largest variation of families ever known. We can say that if there are sufficiently many choices for a sequence family, it becomes difficult to guess the chosen family for someone who don't

know the information about the family. This characteristic is often useful for systems requiring cryptological properties, like LPI property.

3.3 Applications to LPI Signal Design

The concept of LPI (Low-Probability of Interception) signal is considered to face modern physical attacks disturbing communications. Most practical attacks are included into jamming attack or spoofing. Many successive physical attacks for global navigation satellite systems (GNSS) like GPS, has been reported in [53]. In general, an LPI signal is a communication signal having the following characteristics:

1. An invalid user (e. g. attacker) is hard to obtain the communication messages encoded by an LPI signal. In other word, an invalid user cannot find the object of the communication.

2. An invalid user is hard to obtain the information about the structure of the LPI signal. In other word, an invalid user cannot make and transmit resembled signal that may cause confusions to valid receivers.

3. An invalid user is hard to disturb (or interrupt) the communication with an LPI signal. From this, the LPI signal can transmit information more successively in the jamming circumstance in general.

4. An invalid user is hard to determine whether the communication with an LPI signal is operated in specific time. In other word, an invalid user cannot decide the existence of LPI signal in the air.

In general, it is regarded that accomplishing the latter characteristics is harder than the formers. We observe that it is usually accepted that the former characteristics can be accomplished directly if the latter characteristics are accomplished.

The LPI characteristic is useful for commercial and military communications. We show an example requiring the fourth characteristic. Some radar wants to detect enemies without reveals of the existence of the radar signal to enemies. If the LPI property is successive in the case, the radar can get the information about the position of enemies, while the enemies does not realize that they are detected. Examples requiring the third characteristics is more popular, since they contains all the anti-jamming systems, like cellular networks or GNSS systems. On the other hand, the first and second characteristic can be accomplished easily by adopting some cryptography to message or encoder.

The most popular methods to make an LPI signal is using the spread-spectrum techniques. There are mainly two ways for them, one is the direct-sequence spread spectrum (DSSS) and another is the frequency-hopping spread spectrum (FHSS). The direct-sequence spread spectrum uses a sequence $\mathbf{s}$ of sufficient length that is shared to both the transmitter and the receiver(s). The communication is performed by encoding messages with $\mathbf{s}$. For example, the transmitter sends $\mathbf{s}$ if he wants to transmit '0' or sends $-\mathbf{s}$ if he wants to transmit '1'. With the knowledge of them, the receiver uses the matched filter of $\mathbf{s}^H$ to receive the message.

In this system, we can find that the performance is determined by the correlation of the sequence, defined at Definition 1.2, since the correlation value represents the output value of the matched filter of unintended signals. On the other hand, the frequency-hopping spread spectrum works similarly with the DSSS, but the elements of the se-

quence $\mathbf{s}$ do not represent the symbol space of signal. They represents the carrier frequency of the signal. The receiver uses band-pass filters to exclude unintended signals. We can find that the performance in this case is determined by the Hamming correlation of the sequence, defined at Definition 1.4.

Now, we can say that if someone can find a matched filter that is similar with $\mathbf{s}^H$, he also can receive the message. That is, if someone knows about the information of the spreading sequence $\mathbf{s}$, he can obtain the information of the signal. In other word, the LPI characteristic is broken when the attacker guesses $\mathbf{s}$ successively. To show the efficiency of interrupt, we will see the signal-to-interference ratio (SIR) by interference of jamming signal transmitted by an attacker with $\bar{\mathbf{s}}$, that is the sequence guessed by the attacker. The SIR value in this case is in (3.10). Note that the SIR becomes larger in real situation, since the power of the signal transmitted by the attacker is usually higher than the original signal. However, we can say the lower this value becomes, the higher LPI performance is obtained.

$$\mathrm{SIR} = \frac{C(\mathbf{s}, 0)}{\max\limits_{\bar{\mathbf{s}},\tau} C(\mathbf{s}, \bar{\mathbf{s}}, \tau)} \tag{3.10}$$

On the other hand, Equation (3.11) shows the ratio of SNR of attacker who is trying to detect the signal over SNR of valid user. Observe that LPI signals must make this value as low enough.

$$\frac{\mathrm{SNR_A}}{\mathrm{SNR}} = \frac{\max\limits_{\bar{\mathbf{s}},\tau} C(\mathbf{s}, \bar{\mathbf{s}}, \tau)}{C(\mathbf{s}, 0)} = \mathrm{SIR}^{-1} \tag{3.11}$$

To prevent the successive guessing of invalid users, the transmitter must be able to select $\mathbf{s}$ from sufficiently large candidates. However, the number of candidates of sequences having both good auto and cross-correlation characteristics (i.e. Gold or Zadoff-Chu

sequence), is extremely small in general. Many systems supporting LPI characteristic use random sequences encrypted by some cryptographic algorithm to ensure sufficient number of candidates. However, the correlation performance of encrypted sequences is unstable and generally much lower than the preconceived sequences. Many practical systems, like GPS P(Y) or M [22], adopted techniques to overcome unstability of correlation performance, however, these systems also have low average performance.

Our approach from Theorem 3.1 with Theorem 3.6 can make sequence families of perfect autocorrelation characteristic and optimal cross-correlation characteristic, and the variation is sufficiently large. From Theorem 3.8, someone can select $p = 31$ and have $\phi(30)\cdot 31^{30} \approx 2^{152}$ candidates of completely distinct families of sequences with period $31^2 = 961$ and size 30. The number is far larger than the key space of AES-128, that is one of the most widely used cryptography for modern systems requiring security. This means that the brute-force attack to guess $\mathbf{s}$ is almost impossible in this case. Moreover, practical systems using the direct-sequence spread spectrum uses longer sequences. For example, the commercial signals of GPS or Galileo uses spreading sequences of period at least 1023.

Now we propose a system with multiple transmitters or receivers supporting LPI signals. We denote the transmitter as T and n receivers (or users) as $\{U_1, U_2, \cdots, U_n\}$. The transmitter needs to transmit messages $\mathbf{m}_i$ to each receiver U_i in same time, and the signal for some user must not be detected by unintended users, containing another users and attackers. There are two types of keys. All the participants share a group key k_G. Each user U_i has a private key k_i individually, sharing with only the transmitter T.

1. The transmitter T and all users make an agreement for determining an odd prime p that is larger than n, that determines the alphabet size and period of the spreading code.

2. The transmitter selects κ that is relatively prime with $p-1$ using k_G. The selecting method must be shared for all users, so that all the users can make same κ from shared k_G.

3. Each user U_i selects τ_i from zero to $p-1$, and select a sequence $\mathbf{s}_i$ from the associated family $\mathcal{S}(\mathbf{g}[p, \kappa, i, \tau_i])$ using k_i. Two selecting methods must also be shared for all the users.

4. From this, the transmitter has $\mathcal{F} = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n\}$ and each user U_i has $\mathbf{s}_i$.

5. The transmitter send signals $\{\mathbf{m}_1 \otimes \mathbf{s}_1, \mathbf{m}_2 \otimes \mathbf{s}_2, \ldots, \mathbf{m}_n \otimes \mathbf{s}_n\}$. The operation $\otimes$ can be any proper DSSS spreading encoding that is determined by the system.

Observe that $\mathcal{F}$ is an optimal family, so that the noise and the anti-interference performance is also remains to be optimal. Since there are at least $\phi(p-1)p^{p-1}$ candidates, an outside attacker cannot determine any of $\mathbf{s}_i$ by brute-force for sufficiently large p even in the case that he knows p. Another user in the system has the information of κ, so he can obtain the generators of the sequences. Even in this case, there are still at least p^{p-1} candidates.

The system can be adopted to commercial and military communications supporting multiple access requiring anti-jamming characteristic. This can be also applied for the systems with multiple transmitters, like satellites of GNSS systems. In this case, each

transmitter can be corresponded to U_i and all the valid receivers can be corresponded to T.

There may exist more efficient methods for successive guessing at our approach. The cross-correlation of two sequences of same associated family (see Definition def:gen) is generally higher than the cross-correlation of two random sequences. This may indicate that if the attacker knows information about the generator, then some more efficient attack can be found and tried. Someone can determine the generator of sequences in the family of Mow's method [52], since all the generators are equivalent with the Frank-Zadoff's. Note that our method gives many other inequivalent generators, with the number $\phi(p-1)$.

Chapter 4

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 3.6. The number of inequivalent optimal generators of period p with the Hamming correlation property of Theorem 3.3 is also confirmed to be $\varphi(p-1)$ for $p \leq 23$. These results support the following:

Conjecture 4.1 All the optimal generators can be constructed from Theorem 3.6.

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 3.2) while the number of optimal generators from Theorem 3.6 is $p(p-1)\varphi(p-1)$ Now, the number of inequivalent (in the sense of Definition 3.3) perfect generators of period p is $(p-2)!$. All the inequivalent optimal generators which are exhaustively found by computer are shown in Table 4.1 for $p \leq 13$, including their representations of the

Table 4.1: 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

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 4.1 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 3.2). The optimal gener-

ator of a perfect sequence, if it has an optimal generator, may or may not come from Theorem 3.6. It shows a brief summary of Theorems 3.2, 3.3, 3.5 and 3.6. The shaded or dotted area indicates that non-existence has not been proved yet and that no example is currently known either.

Mow [17] 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 3.2 is exactly $p!p^p$. Therefore, if Mow's conjecture is true, then both of the shaded areas outside 'Perfect Generators' in Figure 4.1 will be empty. On the other hand, the truth of Conjecture 4.1 above implies that the inner dotted area becomes empty.

We finalize this chapter with some additional observations for the sequence family from Theorem 3.1 with Theorem 3.6.

Remark 4.1 (Hamming Correlation Property) From the proof of Theorems 3.2 and 3.3, we can easily find that the periodic Hamming autocorrelation of each member of $\mathcal{F}_G(\mathbf{g}(p, \kappa, m, \tau))$ is exactly p for any τ, and the periodic Hamming cross-correlation of any pair is $p-1$ or $p+(p-1)$ for any τ.

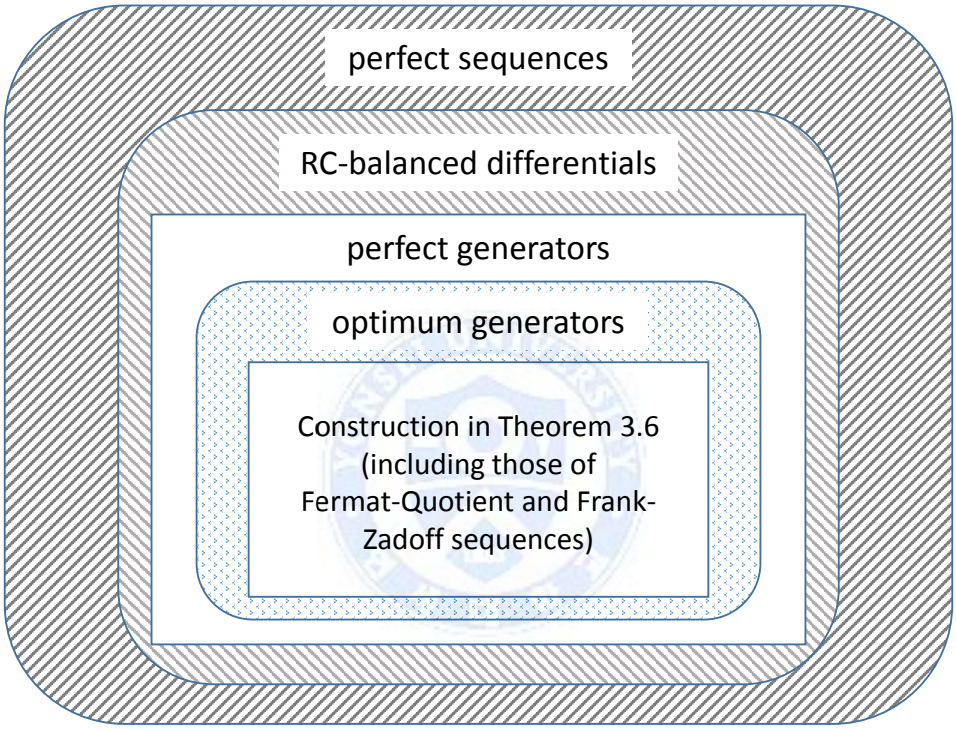

Figure 4.1: Hierarchy of p-ary perfect sequences of period p^2

Bibliography

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

[2] N. Suehiro and M. Hatori, "Modulatable orthogonal sequences and their application to SSMA systems," *IEEE Transactions on Information Theory*, vol. 34, no. 1, pp. 93–100, 1988a.

[3] S. W. Golomb, "Two-valued sequences with perfect periodic autocorrelation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 28, no. 2, pp. 383–386, March 1992.

[4] V. P. Ipatov, "Periodic discrete signals with optimal correlation properties," *Radio I Svyaz*, Moscow, 1992. English translation, ISBN 5-256-00986-9, available from the University of Adelaide, Australia.

[5] N. Zhang and S. W. Golomb, "Polyphase sequences with low autocorrelation," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 1085–1089, May 1993.

[6] H. D. Luke, "Binary Alexis sequences with perfect correlation," *IEEE Transactions on Communications*, vol. 49, no. 6, pp. 966–968, June 2001.

[7] G. Gong and H.-Y. Song, "Two-tuple balance of non-binary sequences with ideal two-level autocorrelation," *Discrete Applied Mathematics*, vol. 154, pp. 2590–2598, 2006.

[8] D. S. Kim, H.-J. Chae, and H.-Y. Song, "A generalization of the family of p-ary decimated sequences with low correlation," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7614–7617, November 2011.

[9] R. C. Heimiller, "Phase shift codes with good periodic correlation propertles," *IRE Transactions on Information Theory*, vol. IT-7, pp. 254–257, October 1961.

[10] R. L. Frank and S. A. Zadoff, "Phase shift pulse codes with good periodic correlation properties," *IRE Transactions on Information Theory (Corresp.)*, vol. IT-S, pp. 381–382, October 1962.

[11] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Transactions on Information Theory*, vol. IT-18, pp. 531–532, July 1972.

[12] B. M. Popović, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1406–1409, July 1992.

[13] D. V. Sarwate, "Bounds on the crosscorrelation and autocorrelation of sequences," *IEEE Transactions on Information Theory*, vol. IT-25, no. 6, pp. 720–724, November 1979.

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

[15] P. Z. Fan and M. Darnell, *Sequence Design for communications applications*. Research Studies Press, 1996.

[16] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory*, vol. Series A 40, pp. 90–107, 1985.

[17] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," *Proceedings of IEEE 4th International Symposium on Spread Spectrum Techniques and Applications, Mainz, Germany*, vol. 3, pp. 955–959, September 1996.

[18] M. Soltanalian and P. Stoica, "On prime root-of-unity sequences with perfect periodic correlation," *IEEE Transactions on Signal Processing*, vol. 62, no. 20, pp. 5458–5470, October 15, 2014.

[19] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, Inc., 2002.

[20] "3GPP TS 36.211 V12.3.0," *3rd Generation Partnership Project; Technical specification group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation (Release 12)*, 2014.

[21] L. Song and J. Shen, *Evolved Cellular Network Planning and Optimization for UMTS and LTE*. CRC Press, 2011.

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

[23] H. Ebner, "Galileo overall architecture definition: SIS frequency characteristics," *GALA-ASTR-DD-019*, no. 5.0, November 2000.

[24] F. F. Kretschmer and K. Gerlach, "Low sidelobe radar waveforms derived from orthogonal matrices," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 27, no. 1, pp. 92–102, January 1991.

[25] R. Chen and B. Cantrell, "Highly bandlimited radar signals," *Proceedings of the 2002 IEEE Radar Conference, Long Beach, CA*, pp. 220–226, April 22-25, 2002.

[26] N. Levanon and E. Mozeson, *Radar Signals*. John Wiley & Sons, Inc., 2004.

[27] R. H. Barker, "Group synchronization of binary digital systems," *in Jackson, W. (ed.), Communication Theory, Academic Press, London*, pp. 273–287, 1953.

[28] L. Bomer and M. Antweiler, "Polyphase Barker sequences," *Electronics Letters*, vol. 25, no. 23, pp. 1577–1579, November 1989.

[29] R. L. Frank, "'polyphase codes with good non-periodic correlation properties," *IEEE Transactions on Information Theory*, vol. IT-9, no. 1, pp. 43–45, January 1963b.

[30] S. W. Golomb and R. A. Scholtz, "Generalized Barker sequences," *IEEE Transactions on Information Theory*, vol. IT-11, no. 4, pp. 533–537, October 1965.

[31] R. Ernvall and T. Metsankyla, "On the p-divisibility of Fermat quotients," *Mathematics of Computation*, vol. 66, pp. 1353–1365, 1997.

[32] Z. Chen, A. Ostafe, and A. Winterhof, "Structure of pseudorandom numbers derived from Fermat quotients," *WAIFI: workshop on the arithmetic of finite fields 2010*, pp. 73–85, 2010.

[33] D. Gomez and A. Winterhof, "Multiplicative character sums of Fermat quotients and pseudorandom sequences," *Periodica Mathematica Hungarica*, vol. 64 (2), pp. 161–168, 2012.

[34] A. Ostafe and I. E. Shparlinski, "Pseudorandomness and dynamics of Fermat quotients," *SIAM J. Discrete Math.*, vol. 25, pp. 50–71, 2011.

[35] M. Su, "New optimum frequency hopping sequences derived from Fermat quotients," *Proceedings of the Sixth International Workshop on Signal Design and Its Applications in Communications (IWSDA 2013), Tokyo, Japan*, pp. 166–169, October 2013.

[36] Z. Chen, "Trace representation and linear complexity of binary sequences derived from fermat quotients," *Science China Information Sciences*, vol. 57, no. 11, pp. 1–10, November 2014.

[37] Z. Chen, X. Du, and R. Marzouk, "Trace representation of pseudorandom binary sequences derived from Euler quotients," *arXiv:1408.2385v1 [cs.CR]*, 2014.

[38] A. Lempel and H. Greenberger, "Families of sequences with optimal hamming

correlation properties," *IEEE Transactions on Information Theory*, vol. 20, pp. 90–94, 1974.

[39] R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequenc hopping sequences: a combinatorial approach," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2408–2420, 2004.

[40] N. C. Beaulieu and D. J. Young, "Designing time-hopping ultrawide bandwidth receivers for multiuser interference enviorments," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 255–284, Feburary 2009.

[41] B. L. Lewis and F. F. Kretschmer, "A new class of polyphase pulse compression codes and techniques," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-17, no. 3, pp. 364–372, May 1981a.

[42] F. F. Kretschmer and B. L. Lewis, "Doppler properties of poly-phase coded pulse compression waveforms," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-19, no. 4, pp. 521–531, July 1983.

[43] N. Levanon and A. Freedman, "Ambiguity function of quadriphase coded radar pulse," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 25, no. 6, pp. 848–853, November 1989.

[44] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," *IBM Journal of Research and Development*, vol. 27, no. 5, pp. 426–431, September 1983.

[45] Y. Liu and P. Fan, "Modified Chu sequences with smaller alphabet size," *Electronics Letters*, vol. 40, no. 10, May 2004.

[46] S. T. Blake and A. Z. Tirkel, "A construction for perfect periodic autocorrelation sequences," *Sequences and Their Applications- SETA 2014*, November 24 to 28, 2014.

[47] S. Ma and W. Ng, "On non-existence of perfect and nearly perfect sequences," *Int. J. Inf. Coding Theory*, vol. 1, no. 1, pp. 15–38, 2009.

[48] E. M. Gabidulin, "Non-binary sequences with the perfect periodic auto-correlation and with optimal periodic cross-correlation," *Proceedings of IEEE International Symposium on Information Theory - ISIT 1993, San Antonio, USA*, 1993.

[49] J. Kang, Y. Whang, B. Ko, and K. Kim, "Generalized cross-correlation properties of Chu sequences," *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 438–444, January 2012.

[50] T.-K. Lee and K. Yang, "The induced correlation of Zadoff-Chu sequences," *Proceedings of IEEE International Symposium on Information Theory - ISIT 2014, Honolulu, USA*, 29 June - 4 July, 2014.

[51] 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," *Proceedings of the IEEE International Symposium on Information Theory - ISIT 2015, Hong-Kong*, June 14-19, 2015.

[52] W. H. Mow, “Unified perfect roots-of-unity sequences construction, and its use for designing better preambles than Zadoff-Chu sequences,” *Proceedings of the Seventh International Workshop on Signal Design and Its Applications in Communications (IWSDA 2015)*, Bengaluru, India, September 13-18, 2015.

[53] C. S. Sin, “Technologies to counter the GPS jamming,” *TTA Journal*, vol. 149, pp. 92–99, 2013.

국 문 요 약

페르마-몫 수열의 완전성에 관한 연구

본 논문은 페르마-몫으로 정의되는 수열이 소수 p에 대해 주기 p^2을 갖는 p진 다중위상수열로 표현될 때 완전한 다중위상수열임을 보인다. 이는 0이 아닌 모든 시간오차에서 수열의 주기 자기상관값이 0이 됨을 의미한다. 본 논문에서는 이러한 수열을 페르마-몫 수열(Fermat-quotient sequence)이라고 정의한다.

또한 본 논문은 페르마-몫 수열을 통해서 만들어지는 수열군이 사와테(Sarwate) 바운드의 관점에서 최적의 상호상관특성을 보이는 것을 확인한다. 여기서 최적이라는 것은 주기 p^2인 수열간 모든 상호 상관값의 최대값이 p가 됨을 의미한다.

본 논문에서 제안한 페르마-몫 수열과 기존에 제안된 프랭크-자도프 수열(Frank-Zadoff sequence)간의 관계를 설명하기 위해 우리는 주기 p^2의 p진 다중위상수열의 생성수열(generator)이라는 개념을 도입하여, p행 p열 크기의 배열 구조로 완전수열을 설명하고 이를 통해 완전수열의 곱으로 이루어진 수열군이 최적 수열군이 되기 위한 조건을 논증한다. 그리고 이러한 조건을

만족할 수 있는 생성수열을 최적 생성수열로 정의한다. 그리하여 이러한 최적 생성수열을 대수적으로 생성할 수 있는 방법을 또 하나의 주요 결과로서 제안한다.

본 논문에서는 마지막으로 이러한 결과로 만들어질 수 있는 최적 수열군이 기존의 프랭크-자도프 수열군과 페르마-몫 수열군은 물론 p가 11 이상일 때는 둘 중 어디에도 포함되지 않는 새로운 최적 수열군을 만들어냄을 확인하고, 이러한 최적 수열군 생성 방법이 매우 많은 서로 다른 최적 수열군을 만들어낼 수 있음을 보인다.

YONSEI UNIVERSITY

핵심되는 말 : 페르마-몫 수열, 프랭크-자도프 수열, 완전한 다중위상수열, 생성수열, 최적수열군, 완전수열의 변환.