Correlation Properties of Fermat-quotient Sequences and related Families

BASED ON

Optimal Families of Perfect Polyphase Sequences from the Array Structure of Fermat-quotient Sequences

IEEE Transactions on Information Theory (2016년 출간예정)




송홍엽

연세대학교 공과대학 전기전자공학부

Communication Signal Design Lab.

Yonsei University

Main Results in this Talk:

- We propose NEW families of
  - p-ary polyphase sequences of period $\mathrm{N} = p^2$ with

    (1) perfect autocorrelation, **zero, for all out-of-phases**

    (2) optimal cross-correlation property $\boldsymbol{p = \sqrt{N}}$**, for all phases**

- To do this, we introduce:
  - The Fermat-quotient sequence, in $\boldsymbol{p \times p}$ **square array** form
  - **Perfectness** from the properties in the array form
  - **Generator**: representing the structure of associated sequences
  - **Conditions** on the generators for perfectness and optimality
  - **Construction of generators** that directly indicates optimal families

Autocorrelation of a Sequence

N is the period of the sequences

Both are p-ary sequences

Correlation of $\boldsymbol{s}$ and $\boldsymbol{m}$ at τ:

$$C(\boldsymbol{s},\boldsymbol{m},\tau)=\sum_{i=0}^{N-1}\omega^{s(i+\tau)-m(i)}$$

$\omega=e^{j\frac{2\pi}{p}}$
Complex primitive
p-th root of unity

- If $\boldsymbol{s}=\boldsymbol{m}$, we call $C(\boldsymbol{s},\boldsymbol{m},\tau)=C(\boldsymbol{s},\tau)$ as autocorrelation of $\boldsymbol{s}$ at τ

- Perfectness of periodic autocorrelation
  - If a binary sequence $\boldsymbol{s}=(0,0,0,1)$ is periodic with period $N=4$, then
    $$C(\boldsymbol{s},1)=\omega^{0-0}+\omega^{0-0}+\omega^{1-0}+\omega^{0-1}=1+1-1-1=0$$
  - Also, $C(\boldsymbol{s},2)=C(\boldsymbol{s},3)=0$

- If $C(\boldsymbol{s},\tau)=0$ for all $0<\tau<N$, we call $\boldsymbol{s}$ as a

Perfect Sequence

$\boldsymbol{s}$ is perfect

Correlation of Two Sequences

- Sarwate bound for perfect sequences
  - If $\boldsymbol{u}$ and $\boldsymbol{v}$ are both **perfect sequences** of period N, then

$$\max_{0 \le \tau < N} |C(\boldsymbol{u}, \boldsymbol{v}, \tau)| \ge \sqrt{N}$$

Theoretical lower bound of cross-correlation

- Sequence pair $\boldsymbol{u}, \boldsymbol{v}$
  - If $\boldsymbol{u}, \boldsymbol{v}$ are perfect sequences of period N for all i and satisfies

$$\max_{0 \le \tau < N} |C(\boldsymbol{u}, \boldsymbol{v}, \tau)| = \sqrt{N}$$

then we call $\boldsymbol{u}, \boldsymbol{v}$ as an

Optimal Pair

Optimal:
achieves the lower bound

- Sequence family $\mathcal{F} = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3, \dots, \boldsymbol{s}_M\}$
  - If $\boldsymbol{s}_i, \boldsymbol{s}_j$ are optimal pairs for all i and $j \ne i$, then we call $\mathcal{F}$ as an

Optimal Family

$\mathcal{F}$ is optimal

Previous Result: Frank-Zadoff

- Frank-Zadoff sequence: $z(t) = \left(t - n\left\lfloor \frac{t}{n} \right\rfloor + 1\right)\left\lfloor \frac{t}{n} + 1 \right\rfloor$

  - n-ary sequence of period $N = n^2$
  - $n \times n$ array form of sequence

$$\boldsymbol{z} = \begin{bmatrix} z(0) & z(1) & z(2) & \cdots & z(n-1) \\ z(n) & z(n+1) & z(n+2) & \cdots & z(2n-1) \\ z(2n) & z(2n+1) & z(2n+1) & \cdots & z(3n-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z((n-1)n) & z((n-1)n+1) & z((n-1)n+2) & \cdots & z(n^2-1) \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 4 & 6 & \cdots & 2n \\ 3 & 6 & 9 & \cdots & 3n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n & 2n & 3n & \cdots & n^2 \end{bmatrix} \pmod{n}$$

  - **Perfect sequence (Frank and Zadoff, 1962)**

  - $\mathcal{F} = \{\boldsymbol{z}, 2\boldsymbol{z}, 3\boldsymbol{z}, \dots, (n-1)\boldsymbol{z}\}$ where n is a prime is an **optimal family (Suehiro, 1988)**

Fermat-quotient Sequence

- Fermat Little Theorem
  - If p is a prime, for any nonzero integer $a < p$,
$$a^{p-1} \equiv 1 \bmod p$$

- Fermat-quotient
$$Q(t) \triangleq \frac{t^{p-1} - 1}{p}$$
  - is always an integer for $t \neq 0 \bmod p$

- Fermat-quotient sequence $\boldsymbol{q} = \{q(0), q(1), \dots\}$

$$q(t) \triangleq \begin{cases} Q(t) \bmod p & \text{if } t \neq 0 \bmod p \\ 0 & \text{otherwise} \end{cases}$$

Examples of FQS

- $p = 5,\ \boldsymbol{q} = \{0,0,3,1,1,0,4,0,4,2,0,3,2,2,3,0,2,4,0,4,0,1,1,3,0\}$

$$\boldsymbol{q} = \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$$

$p \times p$
Array form

Examples of FQS

- $p = 7$
- $\boldsymbol{q} = \{0, 0, 2, 6, 4, 6, 1, 0, 6, 5, 1, 2, 3, 2, 0, 5, 1, 3, 0, 0, 3, 0, 4, 4, 5, 5, 4, 4, 0, 3, 0, 0, 3, 1, 5, 0, 2, 3, 2, 1, 5, 6, 0, 1, 6, 4, 6, 2, 0\}$

$$\boldsymbol{q} = \begin{bmatrix} 0 & 0 & 2 & 6 & 4 & 6 & 1 \\ 0 & 6 & 5 & 1 & 2 & 3 & 2 \\ 0 & 5 & 1 & 3 & 0 & 0 & 3 \\ 0 & 4 & 4 & 5 & 5 & 4 & 4 \\ 0 & 3 & 0 & 0 & 3 & 1 & 5 \\ 0 & 2 & 3 & 2 & 1 & 5 & 6 \\ 0 & 1 & 6 & 4 & 6 & 2 & 0 \end{bmatrix}$$

1. $q(t) = q(p^2 \pm t)$ for all $t = 0,1,2,\ldots$

2. $q(tu^{\pm 1}) = q(t) \pm q(u)$ for all $t, u \neq 0 \pmod{p}$

$q(t) = q(p^2 \pm t)$ for all $t = 0,1,2,\ldots$

When $t \equiv 0 \pmod p$, $t = pk$ some k

$$RHS = q(p^2 \pm pk) = q(p(p \pm k)) = 0 = q(pk) = LHS.$$

When $t \not\equiv 0 \pmod p$,

$$RHS = \frac{1}{p}\left((p^2 \pm t)^{p-1} - 1\right) = \frac{1}{p}\left[\sum_{i=0}^{p-1} \binom{p-1}{i} \cdot (p^2)^i (\pm t)^{p-1-i} - 1\right]$$

$$= \frac{1}{p}\left[(\pm t)^{p-1} - 1 + \underbrace{\sum_{i=1}^{p-1} \binom{p-1}{i} p^{2i} (\pm t)^{p-1-i}}_{\to 0 \pmod p}\right]$$

$$= \frac{1}{p}\left[t^{p-1} - 1\right] \quad \text{(since } p \text{ is odd)}$$

$$= q(t) = LHS.$$

$q(t) = q(p^2 \pm t)$ for all $t = 0,1,2,\ldots$

- $p = 7$

$$\boldsymbol{q} = \begin{bmatrix} \color{blue}{\mathbf{0}} & 0 & 2 & 6 & 4 & 6 & 1 \\ 0 & 6 & 5 & 1 & 2 & 3 & 2 \\ 0 & 5 & 1 & 3 & 0 & 0 & 3 \\ 0 & 4 & 4 & 5 & 5 & 4 & 4 \\ 0 & 3 & 0 & 0 & 3 & 1 & 5 \\ 0 & 2 & 3 & 2 & 1 & 5 & 6 \\ 0 & 1 & 6 & 4 & 6 & 2 & 0 \end{bmatrix}$$

$q(tu^{\pm 1}) = q(t) \pm q(u)$ for all $t, u \neq 0 \pmod p$

First, observe that, for $u \not\equiv 0 \bmod p$

$$q(u^{-1}) = \frac{1}{p}\left[\left(\frac{1}{u}\right)^{p-1} - 1\right] = \frac{1 - u^{p-1}}{p \cdot u^{p-1}} \equiv -\frac{u^{p-1} - 1}{p} \equiv -q(u) \pmod p$$

Therefore,

$$LHS = q(tu^{\pm 1}) = \frac{1}{p}\left[\left(t \cdot u^{\pm 1}\right)^{p-1} - 1\right] = \frac{1}{p}\left[t^{p-1} \cdot (u^{\pm 1})^{p-1} - 1\right]$$

$$= \frac{1}{p}\left[t^{p-1} \cdot (u^{\pm 1})^{p-1} - t^{p-1} - (u^{\pm 1})^{p-1} + 1 \quad + t^{p-1} + (u^{\pm 1})^{p-1} - 2\right]$$

$$= \frac{1}{p}\left[\left(t^{p-1} - 1\right) \cdot \underbrace{\left((u^{\pm 1})^{p-1} - 1\right)}_{\equiv 0 \pmod p} + \left(t^{p-1} - 1\right) + \left((u^{\pm 1})^{p-1} - 1\right)\right]$$

$$\equiv q(t) \pm q(u) \pmod p$$

$q(tu^{\pm 1}) = q(t) \pm q(u)$ for all $t = 0,1,2,\ldots$ and $u \neq 0 \pmod p$

- $p = 7$

$$\boldsymbol{q} = \begin{bmatrix} \mathbf{0} & 0 & 2 & 6 & 4 & 6 & 1 \\ 0 & 6 & 5 & 1 & 2 & 3 & 2 \\ 0 & 5 & 1 & 3 & 0 & 0 & 3 \\ \mathbf{0} & 4 & 4 & 5 & 5 & 4 & 4 \\ 0 & 3 & 0 & 0 & 3 & 1 & 5 \\ 0 & 2 & 3 & 2 & 1 & 5 & 6 \\ \mathbf{0} & 1 & 6 & 4 & 6 & 2 & 0 \end{bmatrix}$$

$u = 3$

$q(3) = 6 = -1$. Therefore,

$$\begin{aligned} t &= 1,2,3,4,5,6, \quad 8,9,10,11,12,13, \quad 15,16,\ldots \\ q(t) &= 0\ 2\ 6\ 4\ 6\ 1 \quad 6\ 5\ 1\ 2\ 3\ 2 \quad 5\ 1\ \ldots \\ q(3t) &= 6\ 1\ 5\ 3\ 5\ 0 \quad 5\ 4\ 0\ 1\ 2\ 1 \quad 4\ 0\ \ldots \end{aligned}$$

Examples of FQS

- $p = 11$

$$\boldsymbol{q} = \begin{bmatrix} 0 & 0 & 5 & 0 & 10 & 7 & 5 & 2 & 4 & 0 & 1 \\ 0 & 10 & 10 & 7 & 7 & 9 & 3 & 5 & 8 & 6 & 2 \\ 0 & 9 & 4 & 3 & 4 & 0 & 1 & 8 & 1 & 1 & 3 \\ 0 & 8 & 9 & 10 & 1 & 2 & 10 & 0 & 5 & 7 & 4 \\ 0 & 7 & 3 & 6 & 9 & 4 & 8 & 3 & 9 & 2 & 5 \\ 0 & 6 & 8 & 2 & 6 & 6 & 6 & 6 & 2 & 8 & 6 \\ 0 & 5 & 2 & 9 & 3 & 8 & 4 & 9 & 6 & 3 & 7 \\ 0 & 4 & 7 & 5 & 0 & 10 & 2 & 1 & 10 & 9 & 8 \\ 0 & 3 & 1 & 1 & 8 & 1 & 0 & 4 & 3 & 4 & 9 \\ 0 & 2 & 6 & 8 & 5 & 3 & 9 & 7 & 7 & 10 & 10 \\ 0 & 1 & 0 & 4 & 2 & 5 & 7 & 10 & 0 & 5 & 0 \end{bmatrix}$$

Third Property of FQS

- $q(t+kp) = q(t) - \frac{k}{t} \quad \text{for } t \neq 0 \bmod p$

$$\boldsymbol{q} = \begin{bmatrix} 0 & q(1) & q(2) & \cdots & q(p-1) \\ 0 & q(1)-1 & q(2)-\frac{1}{2} & \cdots & q(p-1)-\frac{1}{p-1} \\ 0 & q(1)-2 & q(2)-\frac{2}{2} & \cdots & q(p-1)-\frac{2}{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & q(1)-(p-1) & q(2)-\frac{(p-1)}{2} & \cdots & q(p-1)-\frac{(p-1)}{p-1} \end{bmatrix} \pmod p$$

- Each column (except for the left-most) is **balanced**

Every symbol appears exactly the same time in each column except for the left-most column

First Theorem

Theorem 1-1: $\boldsymbol{q}$ is perfect

- p-ary sequence of period p^2

Theorem 1-2: $\mathcal{F}(\boldsymbol{q}) = \{\boldsymbol{q}, 2\boldsymbol{q}, 3\boldsymbol{q}, \ldots, (p-1)\boldsymbol{q}\}$ is optimal

- $m\boldsymbol{q}$ is a sequence from $\boldsymbol{q}$ with all the symbols are multiplied by m

- **Example**: $p = 5$, $\mathcal{F}(\boldsymbol{q}) = \{\boldsymbol{q}, 2\boldsymbol{q}, 3\boldsymbol{q}, 4\boldsymbol{q}\}$

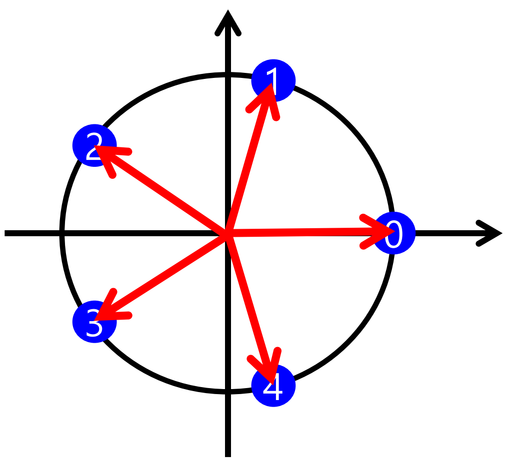
$$\begin{aligned}
\boldsymbol{q} &= (0,0,3,1,1,0,4,0,4,2,0,3,2,2,3,0,2,4,0,4,0,1,1,3,0) \\
2\boldsymbol{q} &= (0,0,1,2,2,0,3,0,3,4,0,1,4,4,1,0,4,3,0,3,0,2,2,1,0) \\
3\boldsymbol{q} &= (0,0,4,3,3,0,2,0,2,1,0,4,1,1,4,0,1,2,0,2,0,3,3,4,0) \\
4\boldsymbol{q} &= (0,0,2,4,4,0,1,0,1,3,0,2,3,3,2,0,3,1,0,1,0,4,4,2,0)
\end{aligned}$$

Difference Sequence

- Define $\boldsymbol{d}_{\boldsymbol{s},\tau}$ as a difference sequence of $\boldsymbol{s}$ by τ as:

$$d_{\boldsymbol{s},\tau}(t) = s(t+\tau) - s(t)$$

- If $\boldsymbol{d}_{\boldsymbol{s},\tau}$ is balanced for all $\tau \neq 0 \bmod N$, then $\boldsymbol{s}$ is perfect
  - $C(\boldsymbol{s},\tau) = \sum \omega^{s(t+\tau)-s(t)} = \sum \omega^{d_{s,\tau}(t)}$
  - Sum of all vertex vectors of a regular polygon



RC-Balancedness

- $p \times p$ array form of $\boldsymbol{d}_{\boldsymbol{s},\tau}$ for p-ary sequence $\boldsymbol{s}$ of period p^2

$$\boldsymbol{d}_{\boldsymbol{s},\tau} = \begin{bmatrix} d_{\boldsymbol{s},\tau}(0) & d_{\boldsymbol{s},\tau}(1) & d_{\boldsymbol{s},\tau}(2) & \cdots & d_{\boldsymbol{s},\tau}(p-1) \\ d_{\boldsymbol{s},\tau}(p) & d_{\boldsymbol{s},\tau}(p+1) & d_{\boldsymbol{s},\tau}(p+2) & \cdots & d_{\boldsymbol{s},\tau}(2p-1) \\ d_{\boldsymbol{s},\tau}(2p) & d_{\boldsymbol{s},\tau}(2p+1) & d_{\boldsymbol{s},\tau}(2p+2) & \cdots & d_{\boldsymbol{s},\tau}(3p-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{\boldsymbol{s},\tau}((p-1)p) & d_{\boldsymbol{s},\tau}((p-1)p+1) & d_{\boldsymbol{s},\tau}((p-1)p+2) & \cdots & d_{\boldsymbol{s},\tau}(p^2-1) \end{bmatrix} \pmod{n}$$

- If (1) each **column** of $\boldsymbol{d}_{\boldsymbol{s},\tau}$ is balanced for all $\tau \neq 0 \bmod p$ and (2) each **row** of $\boldsymbol{d}_{\boldsymbol{s},\tau}$ is balanced for all $\tau \equiv 0 \bmod p$, then we say

$\boldsymbol{s}$ has RC-balanced difference sequences

- If $\boldsymbol{s}$ has RC-balanced difference sequences, then $\boldsymbol{s}$ is perfect
  - Not conversely in general we guess.
  - No proof and **no counterexample** for the converse.

***Theorem 2*: $\boldsymbol{q}$ has RC-balanced difference sequences**

Example of RC-Balancedness

- $\boldsymbol{q} = \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix}$, then

$\boldsymbol{d}_{\boldsymbol{q},1}$	$\boldsymbol{d}_{\boldsymbol{q},2}$	$\boldsymbol{d}_{\boldsymbol{q},3}$	$\boldsymbol{d}_{\boldsymbol{q},4}$	$\boldsymbol{d}_{\boldsymbol{q},5}$
$\begin{bmatrix} 0 & 3 & 3 & 0 & 4 \\ 4 & 1 & 4 & 3 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 2 & 1 & 4 & 1 \\ 1 & 0 & 2 & 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 & 3 & 4 & 3 \\ 0 & 0 & 2 & 1 & 1 \\ 2 & 4 & 1 & 3 & 4 \\ 4 & 3 & 0 & 0 & 2 \\ 1 & 2 & 4 & 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 2 & 3 & 4 \\ 4 & 3 & 0 & 4 & 0 \\ 2 & 0 & 3 & 0 & 1 \\ 0 & 2 & 1 & 1 & 2 \\ 3 & 4 & 4 & 2 & 3 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 1 & 4 & 3 \\ 2 & 1 & 3 & 3 & 0 \\ 3 & 2 & 0 & 2 & 2 \\ 4 & 3 & 2 & 1 & 4 \\ 0 & 4 & 4 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \\ 0 & 4 & 2 & 3 & 1 \end{bmatrix}$

Column-balanced

$\tau \not\equiv 0 \bmod 5$

Row-balanced

$\tau \equiv 0 \bmod 5$

Transformations of Sequences Preserving RC-Balancedness

- ***Lemma***: If $\boldsymbol{s}$ has RC-balanced difference sequences, then

  (1) Constant Multiple: $\boldsymbol{s}' = m\boldsymbol{s}$
  (2) Constant Column Addition: $\boldsymbol{s}' = \mathcal{A}_i(\boldsymbol{s})$
  (3) Column Permutation: $\boldsymbol{s}' = \mathcal{P}_\sigma(\boldsymbol{s})$

  are also have RC-balanced difference sequences

Examples:

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

$$\mathcal{A}_2(\boldsymbol{s}) = \begin{bmatrix} 0 & 0 & 4 & 1 & 1 \\ 0 & 4 & 1 & 4 & 2 \\ 0 & 3 & 3 & 2 & 3 \\ 0 & 2 & 0 & 0 & 4 \\ 0 & 1 & 2 & 3 & 0 \end{bmatrix}$$

$$\mathcal{P}_\sigma(\boldsymbol{s}) = \begin{bmatrix} 0 & 1 & 3 & 0 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 2 & 2 & 3 & 3 \\ 0 & 0 & 4 & 2 & 4 \\ 0 & 3 & 1 & 1 & 0 \end{bmatrix}$$

All of them are RC-balanced !

Optimal Families from FQS

- General form of constant column additions
  - Let $\boldsymbol{a}$ be an integer sequence of period p
  - We denote $\boldsymbol{s}' = \mathcal{A}^{\boldsymbol{a}}(\boldsymbol{s})$ if

$$s'(t) \equiv s(t) + a(t) \bmod p$$

  - $$\mathcal{A}^{\boldsymbol{a}}(\boldsymbol{s}) = \begin{bmatrix} s(0)+a(0) & s(1)+a(1) & \cdots & s(p-1)+a(p-1) \\ s(p)+a(0) & s(p+1)+a(1) & \cdots & s(2p-1)+a(p-1) \\ s(2p)+a(0) & s(2p+1)+a(1) & \cdots & s(3p-1)+a(p-1) \\ \vdots & \vdots & \ddots & \vdots \\ s((p-1)p)+a(0) & s((p-1)p+1)+a(1) & \cdots & s(p^2-1)+a(p-1) \end{bmatrix} \pmod p$$

Theorem 3 :

$$\mathcal{F}_A(\boldsymbol{q}) = \{\mathcal{A}^{\boldsymbol{a}_1}(\boldsymbol{q}), \mathcal{A}^{\boldsymbol{a}_2}(2\boldsymbol{q}), \mathcal{A}^{\boldsymbol{a}_3}(3\boldsymbol{q}), \dots, \mathcal{A}^{\boldsymbol{a}_{p-1}}((p-1)\boldsymbol{q})\}$$

is optimal for any integer sequences $\boldsymbol{a}_i$

Examples (p=3)

Group 1	Group 2
$s = q = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 1 & 0 \end{bmatrix}$	$2s = 2q = \begin{bmatrix} 0 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 2 & 0 \end{bmatrix}$
$\mathcal{A}^{100}(s) = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 2 & 2 \\ 1 & 1 & 0 \end{bmatrix}$	$\mathcal{A}^{020}(2s) = \begin{bmatrix} 0 & 2 & 2 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$
$\mathcal{A}^{002}(s) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}$	$\mathcal{A}^{201}(2s) = \begin{bmatrix} 2 & 0 & 0 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$
$\mathcal{A}^{111}(s) = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix}$	$\mathcal{A}^{220}(2s) = \begin{bmatrix} 2 & 2 & 2 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}$

All the sequences are perfect and any family with two sequences from each group is optimal

Relation with Frank-Zadoff Sequence

- $\mathcal{F}_A(\boldsymbol{z}) = \{\mathcal{A}^{\boldsymbol{a}_1}(\boldsymbol{z}), \mathcal{A}^{\boldsymbol{a}_2}(2\boldsymbol{z}), \mathcal{A}^{\boldsymbol{a}_3}(3\boldsymbol{z}), \dots, \mathcal{A}^{\boldsymbol{a}_{p-1}}((p-1)\boldsymbol{z})\}$ is also **optimal** for any integer sequences $\boldsymbol{a}_i$'s
  - What is the relation of $\boldsymbol{q}$ and $\boldsymbol{z}$?

- **Question:** Is there any other sequence $\boldsymbol{s}$ such that $\mathcal{F}_A(\boldsymbol{s})$ becomes optimal for any integer sequences $\boldsymbol{a}_i$?
  - Most perfect sequences **does not satisfy**,
  - except for $\boldsymbol{q}$, $\boldsymbol{z}$ and their
    - (1) Constant multiples
    - (2) Constant column additions
    - (3) Cyclic shifts and
    - (4) Decimations
      - $\boldsymbol{s}' = \mathcal{D}_d(\boldsymbol{s})$ → $s'(t) = s(dt)$ Ex: (0,1,2,4,3) → (0,2,3,1,4) : d=2
      - $d \neq 0 \bmod p$

- $\boldsymbol{q}$ never goes to $\boldsymbol{z}$ by (1)~(4) and vice versa either

Generator

- Let $\boldsymbol{s}$ be a p-ary sequence of period p^2. If $\boldsymbol{d}_{\boldsymbol{s},p}$ has period p, we let $\boldsymbol{g} = \boldsymbol{d}_{\boldsymbol{s},p}$ and call $\boldsymbol{g}$ as the **generator** of $\boldsymbol{s}$. Then,

Common Differences

- $$\boldsymbol{s} = \begin{bmatrix} s(0) & s(1) & \cdots & s(p-1) \\ s(0)+g(0) & s(1)+g(1) & \cdots & s(p-1)+g(p-1) \\ s(0)+2g(0) & s(1)+2g(1) & \cdots & s(p-1)+2g(p-1) \\ \vdots & \vdots & \ddots & \vdots \\ s(0)+(p-1)g(0) & s(1)+(p-1)g(1) & \cdots & s(p-1)+(p-1)g(p-1) \end{bmatrix}$$
$$= \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} [s(0) \quad s(1) \quad \cdots \quad s(p-1)] + \begin{bmatrix} 1 \\ 2 \\ 3 \\ \vdots \\ p-1 \end{bmatrix} [g(0) \quad g(1) \quad \cdots \quad g(p-1)]$$
$$= \underline{\mathbf{1}}^T \underline{\boldsymbol{s}} + \underline{\boldsymbol{\delta}}^T \underline{\boldsymbol{g}}$$

➢ Also, we say that $\boldsymbol{s}$ has a generator $\boldsymbol{g} = \boldsymbol{d}_{\boldsymbol{s},p}$ if $\boldsymbol{d}_{\boldsymbol{s},p}$ has period p

Example

- Generate a 7-ary sequence of period 49 having

$$\boldsymbol{g} = (0,1,2,3,4,5,6)$$

$\underline{\boldsymbol{s}} \rightarrow$

0	**4**	**3**	**6**	**5**	**1**	**3**
0	1	2	3	4	5	6
0	**5**	**5**	**2**	**2**	**6**	**2**
0	1	2	3	4	5	6
0	**6**	**0**	**5**	**6**	**4**	**1**
0	**0**	**2**	**1**	**3**	**2**	**0**
0	**1**	**4**	**4**	**0**	**0**	**6**
0	**2**	**6**	**0**	**4**	**5**	**5**
0	**3**	**1**	**3**	**1**	**3**	**4**

When we write $t = pi + j$ for $i, j = 0,1,\dots,p-1$, we can write this also as

$$s(t) = s(pi + j) = g(j)i + s(j)$$

Associated Family

- Denote $\mathcal{S}(\boldsymbol{g})$ be the set of all the sequences having the generator $\boldsymbol{g}$
- For any pair $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \mathcal{S}(\boldsymbol{g})$, there exists an integer sequence $\boldsymbol{a}$ of period p that satisfies

$$\boldsymbol{s}_1 = \mathcal{A}^{\boldsymbol{a}}(\boldsymbol{s}_2)$$

- We call $\mathcal{S}(\boldsymbol{g})$ as the associated family of $\boldsymbol{g}$
- The size of $\mathcal{S}(\boldsymbol{g})$ is p^p
  - The number of different choices for $\boldsymbol{a}$
  - Some of them are cyclically equivalent: **the cyclic shift by $\boldsymbol{p}$ of a member is always cyclically equivalent to itself.**

$$\boldsymbol{q} = \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix} \text{--> cyclic shift by } p = 5 \text{ gives } \begin{bmatrix} 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \\ 0 & 0 & 3 & 1 & 1 \end{bmatrix}$$

$\mathrm{g} = 0 \quad 4 \quad 2 \quad 3 \quad 1$

$\mathrm{g} = 0 \quad 4 \quad 2 \quad 3 \quad 1$

Perfect Generator

- We call $\boldsymbol{g}$ as a **perfect generator** if $\boldsymbol{s}$ is perfect for all $\boldsymbol{s} \in \mathcal{S}(\boldsymbol{g})$

Theorem 5: The followings are equivalent:

(1) $\boldsymbol{g}$ is a perfect generator

(2) $\boldsymbol{g}$ is balanced (in a period) (= $\boldsymbol{g}$ is a **permutation**)

(3) Every $\boldsymbol{s} \in \mathcal{S}(\boldsymbol{g})$ has RC-balanced differentials

- The theorem indicates the construction of perfect generator

- The number of p -ary perfect sequences of period p^2:

The number of perfect generators $\quad p!\,p^p \quad$ The number of members in an associated family

= Number of whole p-ary perfect sequences of period p^2 in Mow's conjecture (1996)

Optimal Generator

- **[Another definition]** We call $\boldsymbol{g}$ as an optimal generator if for any $\boldsymbol{s} \in \mathcal{S}(\boldsymbol{g})$,

$$\mathcal{F}_A(\boldsymbol{s}) = \{\mathcal{A}^{\boldsymbol{a}_1}(\boldsymbol{s}), \mathcal{A}^{\boldsymbol{a}_2}(2\boldsymbol{s}), \mathcal{A}^{\boldsymbol{a}_3}(3\boldsymbol{s}), \dots, \mathcal{A}^{\boldsymbol{a}_{p-1}}((p-1)\boldsymbol{s})\}$$

is optimal for any integer sequences $\boldsymbol{a}_i$

Theorem 4: If $\boldsymbol{g}$ is an optimal generator of period p, then

$$\mathcal{F}_G(\boldsymbol{g}) = \left\{\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3, \dots, \boldsymbol{s}_{p-1}\right\}$$

with $\boldsymbol{s}_i \in \mathcal{S}(i\boldsymbol{g})$ **is an optimal family**

Properties of Optimal Generators

Theorem 6 [**A Sufficient Condition for Optimal Generators**]:

$\boldsymbol{g}$ is an optimal generator if

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

for all $\tau = 0,1,2,\ldots,p-1$, and

for any $m, n \neq 0 (mod\ p)$ and $m \neq n\ (mod\ p)$

$H(\boldsymbol{a}, \boldsymbol{b}, \tau)$ is a Hamming correlation of $\boldsymbol{a}$ and $\boldsymbol{b}$ at τ

- Hamming correlation represents the number of hits:

$$\boldsymbol{a} = (0,\boxed{1},2,\boxed{3},4,5,6)$$
$$\boldsymbol{b} = (2,\boxed{1},6,\boxed{3},5,4,0)$$

$$H(\boldsymbol{a}, \boldsymbol{b}, 0) = 2$$
$$H(\boldsymbol{a}, \boldsymbol{b}, 1) = 1$$

$$\boldsymbol{q} = \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix} \text{ where } \boldsymbol{g}(j) = (0\ 4\ 2\ 3\ 1)$$

$$2\boldsymbol{g} = 0\ 3\ 4\ 1\ 2\ 0\ 3\ 4\ 1\ 2$$

$$\boldsymbol{g} = 0\ 4\ 2\ 3\ 1 \qquad \mathbf{H=1}$$

$$\mathcal{T}_4(\boldsymbol{g}) = 0\ 4\ 2\ 3\ 1 \qquad \mathbf{H=1}$$

$$\mathcal{T}_3(\boldsymbol{g}) = 0\ 4\ 2\ 3\ 1 \qquad \mathbf{H=1}$$

$$\mathcal{T}_2(\boldsymbol{g}) = 0\ 4\ 2\ 3\ 1 \qquad \mathbf{H=1}$$

$$\mathcal{T}_1(\boldsymbol{g}) = 0\ 4\ 2\ 3\ 1 \qquad \mathbf{H=1}$$

optimal

Properties of Optimal Generators

Theorem 7: If $\boldsymbol{g}$ is an optimal generator, then

(1) Cyclic Shifts: $\boldsymbol{g}' = \mathcal{T}_\tau(\boldsymbol{g})$
(2) Constant Multiples: $\boldsymbol{g}' = m\boldsymbol{g}$
(3) Decimations: $\boldsymbol{g}' = \mathcal{D}_d(\boldsymbol{g})$

are also optimal generators.

- Example of operations:
  - Cyclic shift: $\mathcal{T}_1(\{0,1,2,3,4\}) = \{1,2,3,4,0\}$
  - Constant multiple: $2\{0,1,2,3,4\} = \{0,2,4,1,3\}$
  - Decimations: $\mathcal{D}_2(\{0,1,2,3,4\}) = \{0,2,4,1,3\}$

Equivalence of Optimal Generators

Optimal generator

Cyclic Shift

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

↓ Constant Multiple

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

↓

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

↓

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

We say they are equivalent if one can be reached from another by (1) and (2).

Decimation and Equivalence

- Decimation is not considered to build the equivalence set of an optimal generator
  - $\mathcal{D}_2(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}) = (0,2,4,1,3) = 2(0,1,2,3,4)$
  - $\mathcal{D}_3(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}) = (0,3,1,4,2) = 3(0,1,2,3,4)$
  - $\mathcal{D}_4(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}) = (0,4,3,2,1) = 4(0,1,2,3,4)$
  - ➔ Equivalent already!

Theorem 8 [**A Sufficient Condition for Theorem 6**]:

If $\boldsymbol{g}$ is balanced and all its decimations are equivalent with $\boldsymbol{g}$, then it satisfies the **Hamming correlation property** in Theorem 6. Hence, it is an optimal generator

Construction of Optimal Generators

Theorem 9 [**Main Contribution**]:

[**The Necessary and Sufficient Condition for Theorem 8**]:

Let $\boldsymbol{g}(\kappa, m, \tau)$ be a p-ary sequence with

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

for any

- integer κ that is relatively prime to $p-1$
- integer $m \neq 0 \bmod p$ **(constant-multiples, one may fix m=1)**
- integer τ **(cyclic-shifts, one may fix τ=0)**

Then, $\boldsymbol{g}(\kappa, m, \tau)$ is a perfect generator and is equivalent with all its decimated sequences, and conversely.

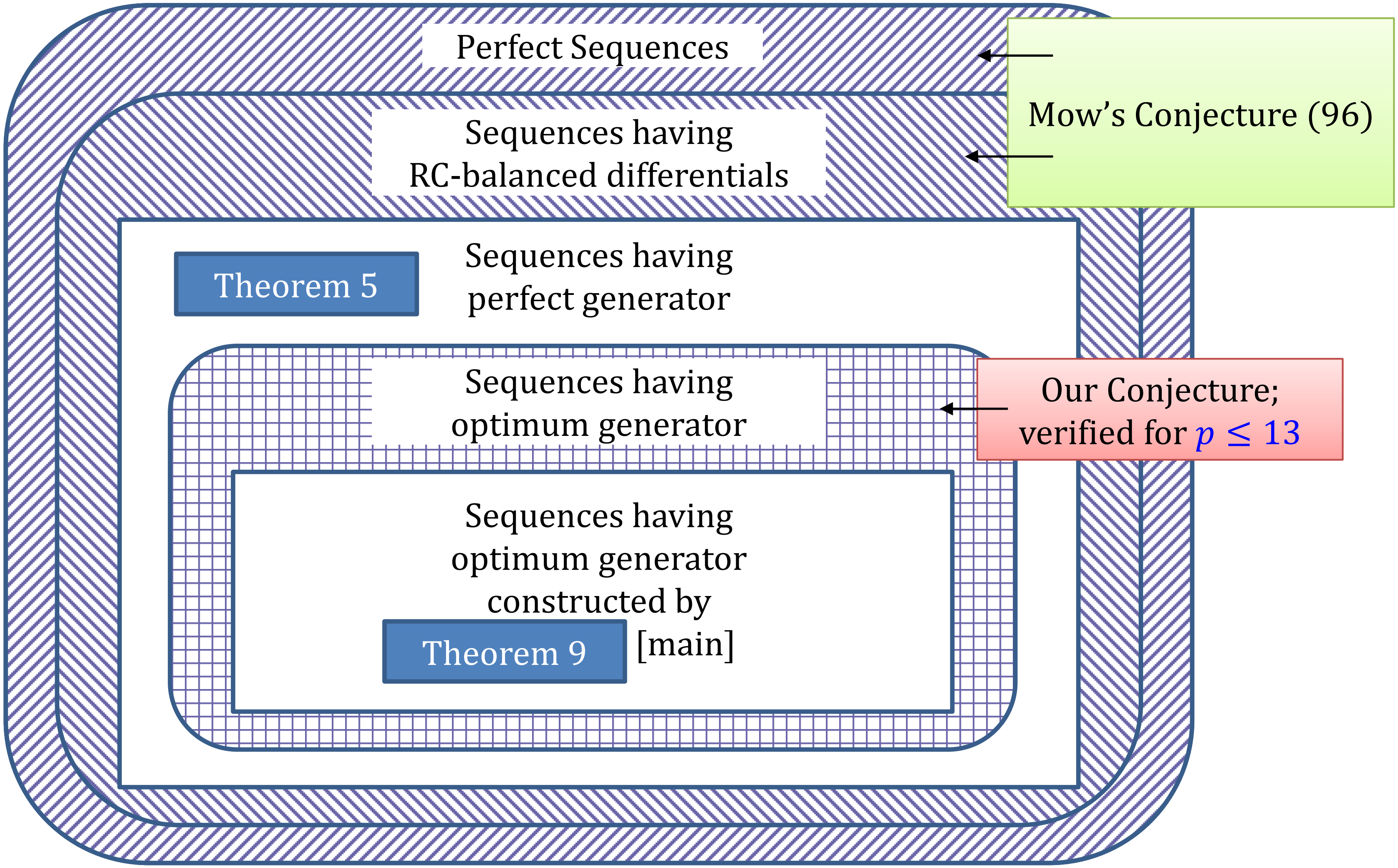
Hence, it is an optimal generator.

All the OGs of $p \leq 13$ ($m = 1, \tau = 0$)

p	Optimum Generator	κ	FQ/FZ
3	{ 0,1,2 }	1	FQ and FZ
5	{ 0,1,2,3,4 }	1	FZ
	{ 0,1,3,2,4 }	3	FQ
7	{ 0,1,2,3,4,5,6 }	1	FZ
	{ 0,1,4,5,2,3,6 }	5	FQ
11	{ 0,1,2,3,4,5,6,7,8,9,10 }	1	FZ
	{ 0,1,8,5,9,4,7,2,6,3,10 }	3	New
	{ 0,1,7,9,5,3,8,6,2,4,10 }	7	New
	{ 0,1,6,4,3,9,2,8,7,5,10 }	9	FQ
13	{ 0,1,2,3,4,5,6,7,8,9,10,11,12 }	1	FZ
	{ 0,1,6,9,10,5,2,11,8,3,4,7,12 }	5	New
	{ 0,1,11,3,4,8,7,6,5,9,10,2,12 }	7	New
	{ 0,1,7,9,10,8,11,2,5,3,4,6,12 }	11	FQ

* FZ: equivalent generator of Frank-Zadoff's FQ: equivalent generator of Fermat-quotient's

Hierarchy of p-ary Perfect Sequences of period p^2



Selected References

- D. C. Chu, ``Polyphase codes with good periodic correlation properties,'' IEEE Trans IT, pp. 531-532, July 1972.
- P. Z. Fan, and M. Darnell, Sequence Design for communications applications, Research Studies Press, 1996.
- R. L. Frank, ``Polyphase codes with good non-periodic correlation properties,'' IEEE Trans IT, pp. 43-45, 1963.
- R. L. Frank and S. A. Zadoff, ``Phase shift pulse codes with good periodic correlation properties,'' IRE Trans IT(Corresp.), vol. IT-S, pp. 381-382, Oct. 1962.
- 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.
- R. C. Heimiller, ``Phase shift codes with good periodic correlation propertles,'' IRE Trans IT, vol. IT-7, pp. 254-257, Oct. 1961.
- D. S. Kim, H.-J. Chae, H.-Y. Song, ``A generalization of the Family of p-ary Decimated Sequences with Low Correlation,'' IEEE Trans IT, vol.57, no.11, pp. 7614-7617, November 2011.
- P. V. Kumar, R. A. Scholtz, and L. R. Welch, ``Generalized bent functions and their properties,'' Journal of Combinatorial Theory, Series A 40, pp. 90-107, 1985.
- N. Levanon and E. Mozeson, Radar Signals, John Wiley & Sons, Inc., 2004.
- W. H. Mow, ``A new unified construction of perfect root-of-unity sequences,'' Proc. IEEE 4th Int. Symp. Spread Spectrum Tech. Appl., Mainz, Germany, vol. 3, pp. 955-959, Sep. 1996.
- 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.
- A. Ostafe and I. E. Shparlinski, ``Pseudorandomness and dynamics of Fermat quotients,'' SIAM J. Discrete Math., vol. 25, pp. 50-71, 2011.
- 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 2015 IEEE International Symposium on Information Theory (ISIT2015), Hong-Kong, June 14-19, 2015.
- B. M. Popovi\'{c}, ``Generalized chirp-like polyphase sequences with optimum correlation properties,'' IEEE Trans IT, vol. 38, no. 4, pp. 1406-1409, July 1992.
- D. V. Sarwate, ``Bounds on the crosscorrelation and autocorrelation of sequences,'' IEEE Trans IT, vol. IT-25, pp. 720-724, 1979.
- M. Soltanalian and P. Stoica, ``On prime root-of-unity sequences with perfect periodic correlation ,'' IEEE Trans SP, vol. 62, 2014.
- N. Suehiro and M. Hatori, ``Modulatable orthogonal sequences and their application to SSMA systems,'' IEEE Trans IT, vol. 34, pp. 93-100, 1988.
- N. Zhang, and S. W. Golomb, ``Polyphase sequences with low autocorrelation,'' IEEE Trans IT, vol. 39, no. 3, pp. 1085-1089, May 1993.