Families of Perfect Polyphase Sequences from the Array Structure of Fermat-Quotient Sequences and Frank-Zadoff Sequences

Ki-Hyeon Park, Hong-Yeop Song, Dae-San Kim

2015 IEEE International Symposium on Information Theory
Hong-Kong
14 ~ 19, June 2015

Communication Signal Design Lab.
Yonsei University

Fermat-Quotient Sequence

- Fermat-quotient

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

  - Integer for $t \neq 0 \bmod p$
  - p is an odd prime

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

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

  - p-ary, period p^2
  - Chen (2010) and Ostafe(2011)

Examples

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

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

$p \times p$
Array form

Examples

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

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

Examples

- $p = 11$

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

Previous Results for Fermat-Quotient Sequences

- A. Ostafe and I. E. Shparlinski, “Pseudorandomness and dynamics of Fermat quotients,” SIAM J. Discrete Math., 2011.

- D. Gomez and A. Winterhof, “Multiplicative Character Sums of Fermat Quotients and Pseudorandom Sequences,” Periodica Mathematica Hungarica, 2012.

- Z. Chen, “Trace representation and linear complexity of binary sequences derived from Fermat quotients,” Science China Information Sciences, Nov. 2014.

- M. Su, “New Optimum Frequency Hopping Sequences Derived From Fermat Quotients,” Proceedings of IWSDA 2013, Oct. 2013.

Main Contribution

- We show that the **Fermat-Quotient sequence** has perfect autocorrelation
  - Zero at any out-of phase
- We propose **NEW** sequence families, including the FQ sequence
  - Individual sequences are perfect
  - Cross-correlation is optimum

Complex Correlation of Sequences

- p-ary, period N, two **integer-represented polyphase sequences**

  $\boldsymbol{u} = (u(0), u(1), \dots)$ and $\boldsymbol{v} = (v(0), v(1), \dots)$

Correlation:

$$C(\boldsymbol{u}, \boldsymbol{v}, \tau) \triangleq \sum_{t=0}^{N-1} \omega^{u(t+\tau) - v(t)}$$

$\omega = e^{j\frac{2\pi}{p}}$

Complex primitive p-th root of unity

- We denote $C(\boldsymbol{u}, \boldsymbol{u}, \tau) = C(\boldsymbol{u}, \tau)$ as autocorrelation of $\boldsymbol{u}$

Perfect Sequence

- A sequence $\boldsymbol{s}$ is called a **<u>perfect sequence</u>** if

$$C(\boldsymbol{s}, \tau) = 0$$

for all $\tau \neq 0 \bmod N$,

<u>Theorem 1-1</u> :

The Fermat Quotient Sequence $\boldsymbol{q}$ is perfect

Sarwate Bound for Cross-Correlation

- Sequence family of size K, sequence length N

- C_A : Maximum magnitude of nontrivial autocorrelation
- C_C : Maximum magnitude of cross-correlation

- Bound (Sarwate, 1979):

$$\frac{C_C^2}{N} + \cancel{\frac{N-1}{N(K-1)}\frac{C_A^2}{N}} \geq 1$$

- For a perfect sequence family,

$$C_C \geq \sqrt{N}$$

Optimum Pair

- A pair $\boldsymbol{u}, \boldsymbol{v}$ is an optimum pair if
  - $\boldsymbol{u}, \boldsymbol{v}$ are **perfect**
  - Satisfies lower bound of Sarwate, that is,

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

Optimum Family

- $\mathcal{F} = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3, \ldots, \boldsymbol{s}_M\}$ is an optimum family if all $\boldsymbol{s}_i, \boldsymbol{s}_j$ are optimum pairs

New Optimum Family

Theorem 1-2 :

$\mathcal{F}(\boldsymbol{q}) = \{\boldsymbol{q}, 2\boldsymbol{q}, 3\boldsymbol{q}, \dots, (p-1)\boldsymbol{q}\}$ is optimum

- $\boldsymbol{s} = m\boldsymbol{q}$ is a sequence with

$$s(i) \equiv mq(i) \bmod p$$

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

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

Frank-Zadoff sequence

- p–ary Frank-Zadoff sequence $\boldsymbol{z}$ of period p^2

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

$$p = 5$$

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

$$p = 7$$

- $\boldsymbol{z}$ is **Perfect** (Frank and Zadoff, 1962)
- $\mathcal{F} = \{\boldsymbol{z}, 2\boldsymbol{z}, 3\boldsymbol{z}, \dots, (n-1)\boldsymbol{z}\}$ is **optimum** (Suehiro, 1988)

Further Investigation

- Observe that
  ① Both FQ and FZ sequences are perfect
  ② All its constant multiples form an optimum family
  ③ They have the same parameters: p–ary, period p^2

FQ Sequence ($p = 5$)

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

$$\boldsymbol{q} = (0,0,3,1,1,0,4,0,4,2,0,3,2,2,3,0,2,4,0,4,0,1,1,3,0)$$
$$2\boldsymbol{q} = (0,0,1,2,2,0,3,0,3,4,0,1,4,4,1,0,4,3,0,3,0,2,2,1,0)$$
$$3\boldsymbol{q} = (0,0,4,3,3,0,2,0,2,1,0,4,1,1,4,0,1,2,0,2,0,3,3,4,0)$$
$$4\boldsymbol{q} = (0,0,2,4,4,0,1,0,1,3,0,2,3,3,2,0,3,1,0,1,0,4,4,2,0)$$

FZ Sequence ($p = 5$)

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

$$\boldsymbol{qz} = (1,2,3,4,0,2,4,1,3,0,3,1,4,2,0,4,3,2,1,0,0,0,0,0,0)$$
$$2\boldsymbol{z} = (2,4,1,3,0,4,3,2,1,0,1,2,3,4,0,3,1,4,2,0,0,0,0,0,0)$$
$$3\boldsymbol{z} = (3,1,4,2,0,1,2,3,4,0,4,3,2,1,0,2,4,1,3,0,0,0,0,0,0)$$
$$4\boldsymbol{z} = (4,3,2,1,0,3,1,4,2,0,2,4,1,3,0,1,2,3,4,0,0,0,0,0,0)$$

Further Investigation

Q1 How are they related?

Q2 In what sense, can they be called “equivalent” with each other?

Q3 Does there any other p–ary perfect sequences of period p^2 with all of whose constant multiples form an optimum family?

➔ All solved and submitted to IT transaction

Differential Sequence and Perfectness

- Define $\boldsymbol{d}_{\boldsymbol{s},\tau}$ as:

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

- $p \times p$ array form of $\boldsymbol{d}_{\boldsymbol{s},\tau}$

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

- ***Theorem 2***: The Fermat-Quotient sequence has $\boldsymbol{d}_{\boldsymbol{q},\tau}$ with

  (1) each <u>column</u> of $\boldsymbol{d}_{\boldsymbol{q},\tau}$ is balanced at $\tau \neq 0 \bmod p$ and

  (2) each <u>row</u> of $\boldsymbol{d}_{\boldsymbol{q},\tau}$ is balanced at $\tau \equiv 0 \bmod p \neq 0$

  - We call this as RC-balanced
  - Hence, perfect
  - This proves Theorem 1-1

Transformations Preserving RC-Balancedness

- *Theorem 3*: If $\boldsymbol{s}$ has RC-balanced differential 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 differential sequences.
  Thus, perfect.

- Can we make optimum pairs using each transforms?
  - (1) makes optimum pairs. Can (2) or (3) give also?

Constant-Column-Addition

- Let $\boldsymbol{s}' = \mathcal{A}_i(\boldsymbol{s})$. Then
$$s'(t) = \begin{cases} s(t) + 1 \bmod p & \text{If } t \equiv i \mod p \\ s(t) & \text{otherwise} \end{cases}$$

- $p \times p$ array form:

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

$$\mathcal{A}_i^j(\boldsymbol{s}) = \begin{bmatrix} s(0) & \cdots & s(i) + j & \cdots & s(p-1) \\ s(p) & \cdots & s(p+i) + j & \cdots & s(2p-1) \\ s(2p) & \cdots & s(2p+i) + j & \cdots & s(3p-1) \\ \vdots & \cdots & \vdots & \ddots & \vdots \\ s((p-1)p) & \cdots & s\big((p-1)p + i\big) + j & \cdots & s(p^2-1) \end{bmatrix} (\bmod p)$$

Combinations of Constant-Column-Addition

- For some integer sequence $\boldsymbol{a} = \big(a(0), a(1), \dots, a(p-1)\big)$,

$$\mathcal{A}^{\boldsymbol{a}}(\boldsymbol{s}) \triangleq \left(\prod_{i=0}^{p-1} \mathcal{A}_i^{a(i)}\right)(\boldsymbol{s})$$

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

Optimum Families

Theorem 4 :

$\boldsymbol{q}$ is FQ and

$\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\boldsymbol{a}_3$, …, $\boldsymbol{a}_{p-1}$ are some integer sequences. Then

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

is optimum

- Theorem 1-2 is a corollary since it is a special case with $\boldsymbol{a}_i = (0,0,..,0)$ for all i

Examples

	$m = \mathbf{1}$ $\boldsymbol{a} = (0,0,0,0,0)$	$m = \mathbf{2}$ $\boldsymbol{a} = (0,0,1,0,0)$	$m = \mathbf{3}$ $\boldsymbol{a} = (2,0,0,0,1)$	$m = \mathbf{4}$ $\boldsymbol{a} = (0,1,2,3,4)$
$m\boldsymbol{q}$	$\begin{bmatrix} 0&0&3&1&1\\0&4&0&4&2\\0&3&2&2&3\\0&2&4&0&4\\0&1&1&3&0 \end{bmatrix}$	$\begin{bmatrix} 0&0&1&2&2\\0&3&0&3&4\\0&1&4&4&1\\0&4&3&0&3\\0&2&2&1&0 \end{bmatrix}$	$\begin{bmatrix} 0&0&4&3&3\\0&2&0&2&1\\0&4&1&1&4\\0&1&2&0&2\\0&3&3&4&0 \end{bmatrix}$	$\begin{bmatrix} 0&0&2&4&4\\0&1&0&1&3\\0&2&3&3&2\\0&3&1&0&1\\0&4&4&2&0 \end{bmatrix}$
$\mathcal{A}^{\boldsymbol{a}}(\boldsymbol{q})$	$\begin{bmatrix} 0&0&3&1&1\\0&4&0&4&2\\0&3&2&2&3\\0&2&4&0&4\\0&1&1&3&0 \end{bmatrix}$	$\begin{bmatrix} 0&0&4&1&1\\0&4&1&4&2\\0&3&3&2&3\\0&2&0&0&4\\0&1&2&3&0 \end{bmatrix}$	$\begin{bmatrix} 2&0&3&1&2\\2&4&0&4&3\\2&3&2&2&4\\2&2&4&0&0\\2&1&1&3&1 \end{bmatrix}$	$\begin{bmatrix} 0&1&0&4&0\\0&0&2&2&1\\0&4&4&0&2\\0&3&1&3&3\\0&2&3&1&4 \end{bmatrix}$
$m\mathcal{A}^{\boldsymbol{a}}(\boldsymbol{q})$	$\begin{bmatrix} 0&0&3&1&1\\0&4&0&4&2\\0&3&2&2&3\\0&2&4&0&4\\0&1&1&3&0 \end{bmatrix}$	$\begin{bmatrix} 0&0&3&2&2\\0&3&2&3&4\\0&1&1&4&1\\0&4&0&0&3\\0&2&4&1&0 \end{bmatrix}$	$\begin{bmatrix} 1&0&4&3&1\\1&2&0&2&4\\1&4&1&1&2\\1&1&2&0&0\\1&3&3&4&3 \end{bmatrix}$	$\begin{bmatrix} 0&4&0&1&0\\0&0&3&3&4\\0&1&1&0&3\\0&2&4&2&2\\0&3&2&4&1 \end{bmatrix}$

: Optimum Family

: Not Optimum

Conclusion

- We proposed **new optimum families** of perfect sequences using the Fermat-Quotient sequence
  - p-ary sequences, period p^2, family size $p-1$
- We showed that Theorem 1~4 work also for the Frank-Zadoff sequences

Some Extra Comments

Q1 How are they related?

Q2 In what sense, can they be called "equivalent" with each other?

Q3 Does there any other p–ary perfect sequences of period p^2 with all of whose constant multiples form an optimum family?

- We distinguished the relation between Fermat-Quotient and Frank-Zadoff sequence
- We argued the equivalence condition to preserve optimality, and showed that FQ and FZ are not equivalent
- We found construction of **general optimal families** of p-ary sequences, period p^2, family size $p-1$ including families not equivalent with both FQ and FZ