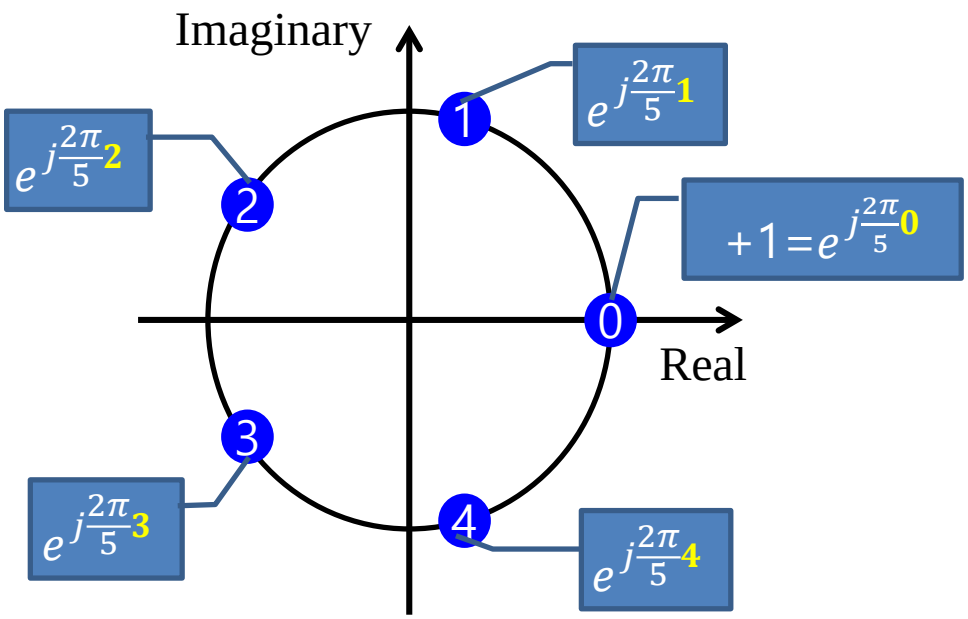
Some new perfect polyphase sequences and optimal families

Hong-Yeop Song
Yonsei University, KOREA

The 5th Sino-Korean International Conference
on Coding Theory and Related Topics
July 2-6, 2018, Shanghai, China

Polyphase sequences

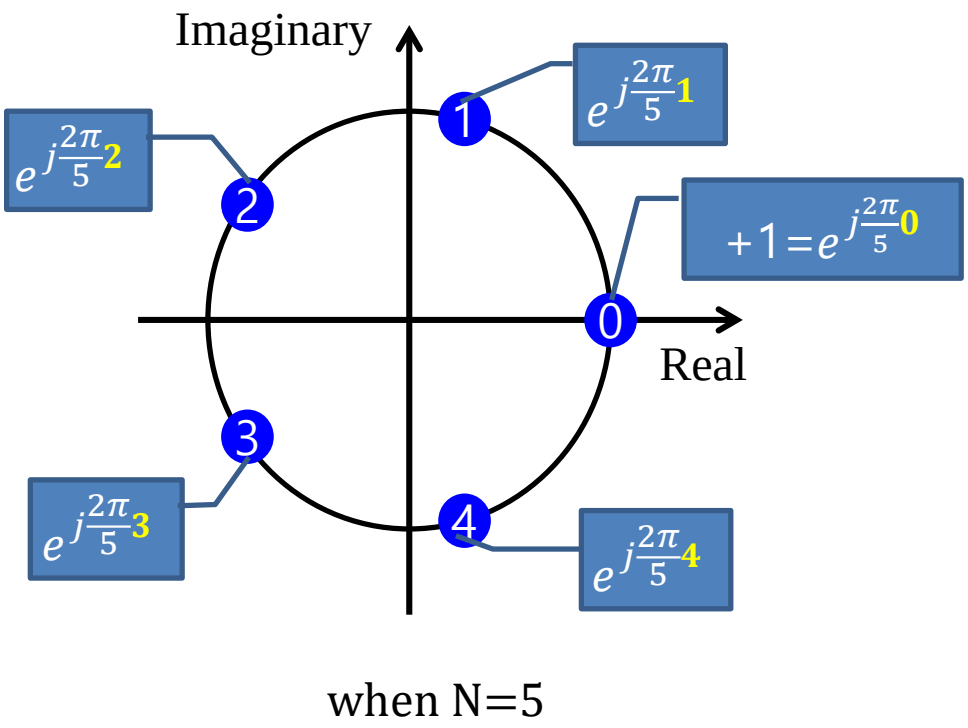
Alphabet of N-ary polyphase sequences



when N=5

Polyphase sequences

Alphabet of N-ary polyphase sequences



when N=5

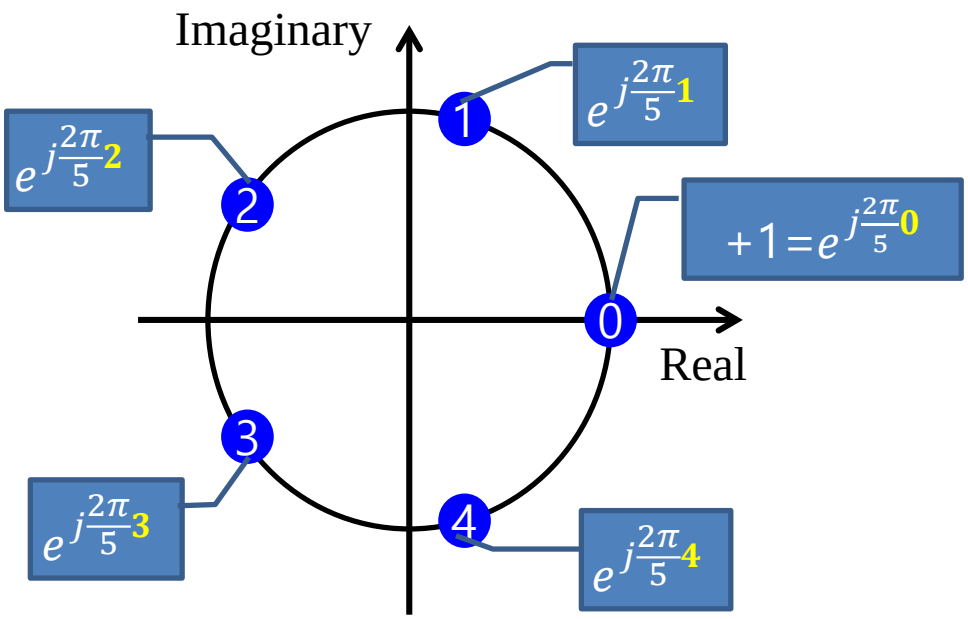
Polyphase sequence representation

- A complex valued sequence

$e^{j\frac{\pi}{5}}, e^{j\frac{3\pi}{5}}, +1, e^{j\frac{2\pi}{5}}, e^{j\frac{4\pi}{5}}, \ldots$

Polyphase sequences

Alphabet of N-ary polyphase sequences



when N=5

Polyphase sequence representation

- A complex valued sequence

$$e^{j\frac{\pi}{5}},\ e^{j\frac{3\pi}{5}},+1,\ e^{j\frac{2\pi}{5}},\ e^{j\frac{4\pi}{5}},\ldots$$

$$1, 3, 0, 2, 4, \ldots$$

- Corresponding phase sequence over the integers **modulo 5**

⇒ It can be equivalently described by its phase sequence

Correlation

- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{L-1}$ and $\boldsymbol{y} = \{y(n)\}_{n=0}^{L-1}$ be two N-ary sequences of length L, then (periodic) correlation between $\boldsymbol{x}$ and $\boldsymbol{y}$ at time shift τ is

$$C_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{n=0}^{L-1} \omega_N^{x(n)} \left(\omega_N^{y(n+\tau)}\right)^* = \sum_{n=0}^{L-1} \omega_N^{x(n)-y(n+\tau)}$$

where $\omega_N = e^{-j\frac{2\pi}{N}}$ is a primitive N-th root of unity.

Correlation

- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{L-1}$ and $\boldsymbol{y} = \{y(n)\}_{n=0}^{L-1}$ be two N-ary sequences of length L, then (periodic) correlation between $\boldsymbol{x}$ and $\boldsymbol{y}$ at time shift τ is

$$C_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{n=0}^{L-1} \omega_N^{x(n)} \left(\omega_N^{y(n+\tau)}\right)^* = \sum_{n=0}^{L-1} \omega_N^{x(n)-y(n+\tau)}$$

where $\omega_N = e^{-j\frac{2\pi}{N}}$ is a primitive N-th root of unity.

  - It is called autocorrelation if $\boldsymbol{y} = \boldsymbol{x}$.
  - It is called cross-correlation otherwise.

Correlation

- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{L-1}$ and $\boldsymbol{y} = \{y(n)\}_{n=0}^{L-1}$ be two N-ary sequences of length L, then (periodic) correlation between $\boldsymbol{x}$ and $\boldsymbol{y}$ at time shift τ is

$$C_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{n=0}^{L-1} \omega_N^{x(n)} \left(\omega_N^{y(n+\tau)}\right)^* = \sum_{n=0}^{L-1} \omega_N^{x(n)-y(n+\tau)}$$

  where $\omega_N = e^{-j\frac{2\pi}{N}}$ is a primitive N-th root of unity.
  - It is called autocorrelation if $\boldsymbol{y} = \boldsymbol{x}$.
  - It is called cross-correlation otherwise.

- A sequence is referred to a '***perfect sequence***' if its autocorrelation is **zero** for any shift $\tau \not\equiv 0 \ (mod\ L)$.

Sarwate bound

- Maximum crosscorrelation magnitude of any two perfect sequences of length L is greater than or equal to $\sqrt{L}$.
  - A pair of two perfect sequences is called an '***optimal pair***' if the pair attains Sarwate bound.
  - A set of perfect sequences is called an '***optimal family***' if any pair of two members in the set attains Sarwate bound.

Sarwate bound

- Maximum crosscorrelation magnitude of any two perfect sequences of length L is greater than or equal to $\sqrt{L}$.
  - A pair of two perfect sequences is called an '***optimal pair***' if the pair attains Sarwate bound.
  - A set of perfect sequences is called an '***optimal family***' if any pair of two members in the set attains Sarwate bound.
- **This is only on the max of cross-correlations. Not on the size of the family, which will be an interesting topic of research.**

In this talk...

- A class of N-ary **perfect polyphase sequences** of period N^2
- **Properties** of **perfect polyphase sequences** and their optimal families

In this talk…

- A class of N-ary **perfect polyphase sequences** of period N^2
- **Properties** of **perfect polyphase sequences** and their optimal families
- **Some constructions** for **optimal families** of N-ary perfect polyphase sequences of period N^2 with respect to **Sarwate bound**

Earlier....

History of constructing perfect polyphase sequences

1960's

Frank, Zadoff
IRE T-IT, 1962
(Heimiller 1961)

1970's

Chu
(Frank,Zadoff)
IEEE T-IT, 1973

1980's

Kumar, Scholtz, Welch
J. Comb. Theory Series A. 1985

Milewski
IBM J. R&D, 1983

Chung, Kumar
IEEE T-IT, 1989

1990's

Popovic
IEEE T-IT, 1992

P1 code
Alphabet size : N
Period : N^2

P2 code
Alphabet size : N
Period : N

P3 code
Alphabet size : N^{k+1}
Period : N^{2k+1}

P4 code
Alphabet size : sN
Period : sN^2

History of constructing perfect polyphase sequences

1960's

Frank, Zadoff
IRE T-IT, 1962
(Heimiller 1961)

1970's

Chu
(Frank,Zadoff)
IEEE T-IT, 1973

1980's

Kumar, Scholtz, Welch
J. Comb. Theory Series A. 1985

Milewski
IBM J. R&D, 1983

Chung, Kumar
IEEE T-IT, 1989

1990's

Popovic
IEEE T-IT, 1992

P1 code
Alphabet size : N
Period : N^2

P2 code
Alphabet size : N
Period : N

P3 code
Alphabet size : N^{k+1}
Period : N^{2k+1}

P4 code
Alphabet size : sN
Period : sN^2

Mow's two unified construction (dissertation 1993, ISSTA 1996)

P1 codes

N-ary Frank sequence of period N^2
(Frank and Zadoff)

$$\mathcal{I}\left(\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & N-1 \\ 0 & 2 & 4 & \cdots & 2(N-1) \\ 0 & 3 & 6 & \cdots & 3(N-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & (N-1) & 2(N-1) & \cdots & (N-1)^2 \end{bmatrix}\right)$$

$$= \mathcal{I}\left(\begin{bmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ N-1 \end{bmatrix}\begin{bmatrix} 0 & 1 & 2 & \cdots & N-1 \end{bmatrix}\right)$$

$$= \mathcal{I}\left(\underline{\delta}_N^T \underline{\delta}_N\right)$$

Where $\mathcal{I}(\boldsymbol{X})$ stands for the operation that generates a sequences by reading X row-by-row,

P1 codes

N-ary Frank sequence of period N^2
(Frank and Zadoff)

$$\mathcal{I}\left(\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & N-1 \\ 0 & 2 & 4 & \cdots & 2(N-1) \\ 0 & 3 & 6 & \cdots & 3(N-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & (N-1) & 2(N-1) & \cdots & (N-1)^2 \end{bmatrix}\right)$$

$$= \mathcal{I}\left(\begin{bmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ N-1 \end{bmatrix}\begin{bmatrix} 0 & 1 & 2 & \cdots & N-1 \end{bmatrix}\right)$$

$$= \mathcal{I}\left(\underline{\delta}_N^T \underline{\delta}_N\right)$$

Generalization

N-ary generalized Frank sequence of period N^2
(Kumar, Sholtz, and Welch)

$$\mathcal{I}\left(\begin{bmatrix} 0 \\ 1 \\ 2 \\ \vdots \\ N-1 \end{bmatrix}\underline{g} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}\underline{m}\right)$$

$$= \mathcal{I}\left(\underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}\right)$$

$\underline{g}$: a N-tuple that is a permutation over $\mathbb{Z}_N$

$\underline{m}$: any N-tuple

Where $\mathcal{I}(\boldsymbol{X})$ stands for the operation that generates a sequences by reading X row-by-row,

$\underline{\delta}_N \triangleq [0 \quad 1 \quad 2 \quad \cdots \quad N-1]$, and $\underline{1}_N = [\underbrace{1 \quad 1 \quad 1 \quad \cdots \quad 1}_{N \text{ times}}]$

Example $(N = 5)$

Frank sequence

For $\underline{g} = \underline{\delta}_5 = [0\ \ 1\ \ 2\ \ 3\ \ 4]$,

$$\underline{\delta}_5^T \underline{g} = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} [0\ \ 1\ \ 2\ \ 3\ \ 4] = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{bmatrix}$$

Interleaving operation $\mathcal{I}$ (read row-by-row)

$\{0, 0, 0, 0, 0, 0, 1, 2, 3, 4, 0, 2, 4, 1, 3, 0, 3, 1, 4, 2, 0, 4, 3, 2, 1\}$

Example ($N = 5$)

Frank sequence

For $\underline{g} = \underline{\delta}_5 = [0\ \ 1\ \ 2\ \ 3\ \ 4]$,

$$\underline{\delta}_5^T \underline{g} = \begin{bmatrix}0\\1\\2\\3\\4\end{bmatrix}[0\ \ 1\ \ 2\ \ 3\ \ 4] = \begin{bmatrix}0&0&0&0&0\\0&1&2&3&4\\0&2&4&1&3\\0&3&1&4&2\\0&4&3&2&1\end{bmatrix}$$

Interleaving operation $\mathcal{I}$ (read row-by-row)

$\{0,0,0,0,0,0,1,2,3,4,0,2,4,1,3,0,3,1,4,2,0,4,3,2,1\}$

Generalized Frank sequence

For $\underline{g} = [0\ 1\ 4\ 3\ 2]$, $\underline{m} = [0\ 0\ 1\ 3\ 2]$,

$$\underline{\delta}_5^T \underline{g} + \underline{1}_N^T \underline{m} = \begin{bmatrix}0\\1\\2\\3\\4\end{bmatrix}[0\ \ 1\ \ 4\ \ 3\ \ 2] + \begin{bmatrix}1\\1\\1\\1\\1\end{bmatrix}[0\ \ 0\ \ 1\ \ 3\ \ 2] = \begin{bmatrix}0&0&1&3&2\\0&1&0&1&4\\0&2&4&4&1\\0&3&3&2&3\\0&4&2&0&0\end{bmatrix}$$

Interleaving operation $\mathcal{I}$ (read row-by-row)

$\{0,0,1,3,2,0,1,0,1,4,0,2,4,4,1,0,3,3,2,3,0,4,2,0,0\}$

Constructing Optimal Families from P1 codes

P1 codes

Frank sequence
and its modulations
$\mathcal{I}\left(\underline{\delta}_N^T \underline{\delta}_N + \underline{1}_N^T \underline{m}\right)$
(Frank/Zadoff)

Suehiro and Hatori, IEEE T-IT, 1988 :
by using multiplying some constants to the sequence

Optimal Families of
Frank sequences

Constructing Optimal Families from P1 codes

P1 codes

Frank sequence and its modulations

$\mathcal{I}\left(\underline{\delta}_N^T \underline{\delta}_N + \underline{1}_N^T \underline{m}\right)$

(Frank/Zadoff)

Suehiro and Hatori, IEEE T-IT, 1988 :

by using multiplying some constants to the sequence

Two different approaches

Mow, IEEE T-COM, 1995

(Alltop IEEE T-IT, 1984)

by using decimations

Optimal Families of Frank sequences

Constructing Optimal Families from P1 codes

???

Generalized Frank sequences (Kumar/Scholtz/Welch)

P1 codes

Suehiro and Hatori, IEEE T-IT, 1988 :

by using multiplying some constants to the sequence

Optimal Families of generalized Frank sequences

(N=odd prime: 2016 T-IT)

(N=odd integer:2018 T-IT)

Frank sequence and its modulations

$\mathcal{I}\left(\underline{\delta}_N^T \underline{\delta}_N + \underline{1}_N^T \underline{m}\right)$

(Frank/Zadoff)

Two different approaches

Optimal Families of Frank sequences

Mow, IEEE T-COM, 1995

(Alltop IEEE T-IT, 1984)

by using decimations

Brief review of two constructions

Suehiro and Hatori 1988

$\mathcal{U} \triangleq \{u_i \in \mathbb{Z}_N \mid \gcd(u_i, N) = 1, u_i \not\equiv u_j \text{ if } i \neq j, \gcd(u_i - u_j, N) = 1\}$

$\underline{m}_1, \underline{m}_2, \ldots, \underline{m}_{|\mathcal{U}|}$: **arbitrary** chosen N-tuples.

Optimal family $S = \{\mathcal{I}(\underline{\delta}_N^T u_i \underline{\delta}_N + \underline{1}_N^T \underline{m}_i) \mid u_i \in \mathcal{U}\}$

Modulatable sequences
(by Suehiro and Hatori)

Mow 1995 (Alltop 1984, N prime)

$\mathcal{U} \triangleq \{u_i \in \mathbb{Z}_N \mid \gcd(u_i, N) = 1, u_i \not\equiv u_j \text{ if } i \neq j, \gcd(u_i - u_j, N) = 1\}$

$\underline{m}_1, \underline{m}_2, \ldots, \underline{m}_{|\mathcal{U}|}$: **arbitrary** chosen N-tuples.

Optimal family $S = \{\mathfrak{D}_d(\mathcal{I}(\underline{\delta}_N^T \underline{\delta}_N + \underline{1}_N^T \underline{m}_i)) \mid d \in \mathcal{U}\}$

where $\mathfrak{D}$ is decimation operator.

Optimal Families of Perfect Polyphase Sequences from Fermat-Quotient Sequences




K.-H Park, H.-Y. Song, D. S. Kim, and Solomon W. Golomb,

IEEE Trans. on Inf. Theory,
Feb. 2016.

Fermat-Quotient sequence is perfect

- **Definition. (Fermat-quotient sequence)**

  For an odd prime p, the Fermat-quotient sequence $\boldsymbol{q} = \{q(n)\}_{n=0}^{p^2-1}$ over $\mathbb{Z}_p$ is defined by

$$q(n) = \begin{cases} \dfrac{n^{p-1}-1}{p} \pmod p & \text{if } n \not\equiv 0 \pmod p \\ 0 & \text{otherwise.} \end{cases}$$

Fermat-Quotient sequence is perfect

- **Definition. (Fermat-quotient sequence)**

  For an odd prime p, the Fermat-quotient sequence $\boldsymbol{q} = \{q(n)\}_{n=0}^{p^2-1}$ over $\mathbb{Z}_p$ is defined by

$$q(n) = \begin{cases} \dfrac{n^{p-1}-1}{p} \pmod p & \text{if } n \not\equiv 0 \pmod p \\ 0 & \text{otherwise.} \end{cases}$$

- **Theorem.**

  For any odd prime p, the p-ary Fermat-quotient sequence $\boldsymbol{q}$ of period p^2 is perfect.

Generators and associated families

- The Fermat quotient sequence has the following structure

$$\mathcal{I}\left(\underline{\delta}_p^T \underline{g} + \underline{1}_p^T \underline{m}\right).$$

Example) $\boldsymbol{q} \Leftrightarrow \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} [0, 4, 2, 3, 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} [0, 0, 3, 1, 1]$

  - Therefore, it is a subclass of the generalized Frank sequences.

Generators and associated families

- The Fermat quotient sequence has the following structure

$$\mathcal{I}\left(\underline{\delta}_p^T \underline{g} + \underline{1}_p^T \underline{m}\right).$$

Example) $\boldsymbol{q} \Leftrightarrow \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} [0, 4, 2, 3, 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} [0, 0, 3, 1, 1]$

  - Therefore, it is a subclass of the generalized Frank sequences.
  - We call $\underline{g}$ a **generator**.

Generators and associated families

- The Fermat quotient sequence has the following structure

$$\mathcal{I}\left(\underline{\delta}_p^T \underline{g} + \underline{1}_p^T \underline{m}\right).$$

Example) $\boldsymbol{q} \Leftrightarrow \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} [0, 4, 2, 3, 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} [0, 0, 3, 1, 1]$

  - Therefore, it is a subclass of the generalized Frank sequences.
  - We call $\underline{g}$ a **generator**.
  - We call a collection of all the possible sequences for a fixed $\underline{g}$ an **associated family** of $\underline{g}$ and denote it by $\mathcal{S}(\underline{g})$.

  That is, $\mathcal{S}(\underline{g})$ is the set of all the modulations of $\mathcal{I}\left(\underline{\delta}_p^T \underline{g}\right)$

In general…

- **Definition. (Perfect generators)**
  A generator $\underline{g}$ is a perfect generator
  if all the sequences $\boldsymbol{s} \in \mathcal{S}(\underline{g})$ are perfect.

- Known fact: All the generators of the **generalized Frank sequences** are perfect generators
  - Is there any other perfect generator?

In general…

- **Definition. (Perfect generators)**
  A generator $\underline{g}$ is a perfect generator
  if all the sequences $\boldsymbol{s} \in \mathcal{S}(\underline{g})$ are perfect.

- Known fact: All the generators of the **generalized Frank sequences** are perfect generators
  - Is there any other perfect generator?

- **Theorem. (Perfect generator construction)**
  The followings are equivalent.
  1) $\underline{g}$ is perfect generator.
  2) $\underline{g}$ is a permutation of $\mathbb{Z}_p$.

In general…

- **Definition. (Perfect generators)**
  A generator $\underline{g}$ is a perfect generator
  if all the sequences $\boldsymbol{s} \in \mathcal{S}(\underline{g})$ are perfect.

- Known fact: All the generators of the **generalized Frank sequences** are perfect generators
  - Is there any other perfect generator?

- **Theorem. (Perfect generator construction)**
  The followings are equivalent.
  1) $\underline{g}$ is perfect generator.
  2) $\underline{g}$ is a permutation of $\mathbb{Z}_p$.

For odd prime length, there is no other perfect generators!

Transformations

- **Definition.**
  Let $\underline{g}$ be a generator of length p.
  1) **(cyclic shifts) Shifting $\underline{g}$ cyclically to the left by τ.**
  2) **(constant multiples) multiplying all the elements of $\underline{g}$ by an integer $u \not\equiv 0 \pmod{p}$.**
  3) **(Decimations) Decimating $\underline{g}$ by an integer $d \not\equiv 0 \pmod{p}$.**
  - With an abuse, we use these transformations for sequences.

- **Corollary.**
  Let $\underline{g}$ be a perfect generator of length p.
  1) Any constant multiple of $\underline{g}$ is also a perfect generator.
  2) Any decimation of $\underline{g}$ is also a perfect generator.

Optimal family of perfect sequences

A given **perfect generator** $\underline{g}$ of odd prime length p

$$\mathcal{U} = \{u_i | \gcd(u_i, p) = 1 = \gcd(u_i - u_j, p), i \neq \mathrm{j}\}.$$

Optimal family of perfect sequences

A given **perfect generator** $\underline{g}$ of odd prime length p

$$\mathcal{U} = \{u_i \,|\, \gcd(u_i, p) = 1 = \gcd(u_i - u_j, p), i \neq \mathrm{j}\}.$$

Make associated families

$\mathcal{S}(u_1\underline{g})$ $\mathcal{S}(u_2\underline{g})$

Optimal family of perfect sequences

A given **perfect generator** $\underline{g}$ of odd prime length p

$$\mathcal{U} = \{u_i \,|\, \gcd(u_i, p) = 1 = \gcd(u_i - u_j, p), i \neq \mathrm{j}\}.$$

Make associated families

$$\mathcal{S}(u_1\underline{g}) \quad \mathcal{S}(u_2\underline{g}) \quad \mathcal{S}(u_3\underline{g}) \quad \cdots \quad \mathcal{S}(u_{p-1}\underline{g})$$

Optimal family of perfect sequences

A given **perfect generator** $\underline{g}$ of odd prime length p

$$\mathcal{U} = \{u_i \,|\, \gcd(u_i, p) = 1 = \gcd(u_i - u_j, p), i \neq \mathrm{j}\}.$$

Make associated families

$\mathcal{S}(u_1\underline{g})$ $\mathcal{S}(u_2\underline{g})$ $\mathcal{S}(u_3\underline{g})$ … $\mathcal{S}(u_{p-1}\underline{g})$

Pick a sequence from each $\mathcal{S}(u_i\underline{g})$

An optimal family $\mathcal{F}(\underline{g})$ of p-ary **perfect sequences** of period p^2

Optimal family of perfect sequences

A given **perfect generator** $\underline{g}$ of odd prime length p

optimal generator

$$\mathcal{U} = \{u_i \,|\, \gcd(u_i, p) = 1 = \gcd(u_i - u_j, p), i \neq \mathrm{j}\}.$$

Make associated families

$\mathcal{S}(u_1\underline{g})$ $\mathcal{S}(u_2\underline{g})$ $\mathcal{S}(u_3\underline{g})$ … $\mathcal{S}(u_{p-1}\underline{g})$

Pick a sequence from each $\mathcal{S}(u_i\underline{g})$

An optimal family $\mathcal{F}(\underline{g})$ of p-ary **perfect sequences** of period p^2

Optimal family of perfect sequences

A given **perfect generator** $\underline{g}$ of odd prime length p ?

optimal generator

$$\mathcal{U} = \{u_i \,|\, \gcd(u_i, p) = 1 = \gcd(u_i - u_j, p), i \neq j\}.$$

Make associated families

$\mathcal{S}(u_1\underline{g})$ $\mathcal{S}(u_2\underline{g})$ $\mathcal{S}(u_3\underline{g})$ … $\mathcal{S}(u_{p-1}\underline{g})$

Pick a sequence from each $\mathcal{S}(u_i\underline{g})$

An optimal family $\mathcal{F}(\underline{g})$ of p-ary **perfect sequences** of period p^2 ?

Optimal generators

- **Definition. (optimal generators)**
  A (perfect) generator $\underline{g}$ is a **optimal generator** if any pair of $\boldsymbol{x} \in \mathcal{S}(m\underline{g})$ and $\boldsymbol{y} \in \mathcal{S}(n\underline{g})$ is an **optimal pair** for any non-zero m, n with $m \not\equiv n \pmod{\boldsymbol{p}}$.

Optimal generators

- **Definition. (optimal generators)**
  A (perfect) generator $\underline{g}$ is a **optimal generator** if any pair of $\boldsymbol{x} \in \mathcal{S}(m\underline{g})$ and $\boldsymbol{y} \in \mathcal{S}(n\underline{g})$ is an **optimal pair** for any non-zero m, n with $m \not\equiv n \pmod{\boldsymbol{p}}$.

- In the previous, we indeed showed that
  the generator of Fermat-quotient sequence is an optimal generator.

- And, from the result due to Suehiro and Hatori, we know that
  the generator of the original Frank sequence is also an optimal generator.

- Is there any other optimal generators of odd prime length?

Algebraic construction

For an odd prime p, let $\underline{g}_{m,\tau,\kappa}$ be a p-tuple over $\mathbb{Z}_p$ where its n-th term, denoted by $g(n; m, \tau, \kappa)$, is given by

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

where κ is an integer coprime to $p - 1$,

$m \not\equiv 0 \pmod{p}$, and τ is an integer.

Algebraic construction

Theorem.

For an odd prime p, let $\underline{g}_{m,\tau,\kappa}$ be a p-tuple over $\mathbb{Z}_p$

where its n-th term, denoted by $g(n; m, \tau, \kappa)$, is given by

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

where κ is an integer coprime to $p - 1$,

$m \not\equiv 0 \pmod{p}$, and τ is an integer.

Then, $\underline{g}$ is an optimal generator of length p

Algebraic construction

Theorem.

For an odd prime p, let $\underline{g}_{m,\tau,\kappa}$ be a p-tuple over $\mathbb{Z}_p$ where its n-th term, denoted by $g(n; m, \tau, \kappa)$, is given by

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

where κ is an integer coprime to $p - 1$,

$m \not\equiv 0 \pmod{p}$, and τ is an integer.

Then, $\underline{g}$ is an optimal generator of length p.

- Two optimal generators $\underline{g}_{m,\tau,\kappa}$ and $\underline{g}_{m',\tau',\kappa'}$ are **equivalent if and only if** $\kappa \equiv \kappa' \pmod{p-1}$.

Algebraic construction

Theorem.

For an odd prime p, let $\underline{g}_{m,\tau,\kappa}$ be a p-tuple over $\mathbb{Z}_p$ where its n-th term, denoted by $g(n; m, \tau, \kappa)$, is given by

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

where κ is an integer coprime to $p - 1$,

$m \not\equiv 0 \pmod{p}$, and τ is an integer.

Then, $\underline{g}$ is an optimal generator of length p.

- Two optimal generators $\underline{g}_{m,\tau,\kappa}$ and $\underline{g}_{m',\tau',\kappa'}$ are **equivalent if and only if** $\kappa \equiv \kappa' \pmod{p-1}$.
- Therefore, only $\boldsymbol{\phi(p-1)}$ **inequivalent optimal generators** of **length** $\boldsymbol{p}$.

Inequivalent optimal generators with $m = 1, \tau = 0$

p	optimal generators (representatives)	κ
3	$\{0,1,2\}$ **(Frank) (FQ)**	1
5	$\{0,1,2,3,4\}$ **(Frank)**	1
	$\{0,1,3,2,4\}$ **(FQ)**	3
7	$\{0,1,2,3,4,5,6\}$ **(Frank)**	1
	$\{0,1,4,5,2,3,6\}$ **(FQ)**	5
11	$\{0,1,2,3,4,5,6,7,8,9,10\}$ **(Frank)**	1
	$\{0,1,6,4,3,9,2,8,7,5,10\}$ **(FQ)**	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	$\{0,1,2,3,4,5,6,7,8,9,10,11,12\}$ **(Frank)**	1
	$\{0,1,6,9,10,5,2,11,8,3,4,7,12\}$	5
	$\{0,1,7,9,10,8,11,2,5,3,4,6,12\}$ **(FQ)**	11
	$\{0,1,11,3,4,8,7,6,5,9,10,2,12\}$	7

A construction of odd length generators for optimal families of perfect sequences

M. K. Song and H.-Y. Song,

IEEE Trans. on Inf. Theory
(April. 2018, Special Issue)

Perfect generators of any length

- We now extend the previous results by considering

$$\mathcal{I}\left(\underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}\right),$$

where N is an odd integer and $\underline{g}, \underline{m}$ are of length N.

Perfect generators of any length

- We now extend the previous results by considering

$$\mathcal{I}\left(\underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}\right),$$

where N is an odd integer and $\underline{g}, \underline{m}$ are of length N.

- **Definition**. (Perfect generators)
  A generator $\underline{g}$ of length N is a perfect generator
  if any sequence in its associated family $\mathcal{S}(\underline{g})$ is perfect.

Perfect generators of any length

- We now extend the previous results by considering

$$\mathcal{I}\left(\underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}\right),$$

where N is an odd integer and $\underline{g}, \underline{m}$ are of length N.

- **Definition**. (Perfect generators)
A generator $\underline{g}$ of length N is a perfect generator
if any sequence in its associated family $\mathcal{S}(\underline{g})$ is perfect.

- Obviously, a generator of any N-ary generalized Frank sequences of period N^2 is a perfect generator.

Optimal generators of odd length

- **Definition. (optimal generators of odd lengths)**
  A (perfect) generator $\underline{g}$ is a optimal generator if any pair of $\boldsymbol{x} \in \mathcal{S}(\underline{g})$ and $\boldsymbol{y} \in \mathcal{S}(u\underline{g})$ is an optimal pair **for any u** such that **both u and $u-1$ are coprime to N.**

Optimal generators of odd length

- **Definition. (optimal generators of odd lengths)**
  A (perfect) generator $\underline{g}$ is a optimal generator if any pair of $\boldsymbol{x} \in \mathcal{S}(\underline{g})$ and $\boldsymbol{y} \in \mathcal{S}(u\underline{g})$ is an optimal pair **for any u** such that **both u and $u-1$ are coprime to N.**

- Non-existence of an **even-length optimal generator** can be proved easily.

Optimal family construction

A given optimal generator $\underline{g}$ of odd length N

$$\mathcal{U} = \{u_i \,|\, \gcd(u_i, N) = 1 = \gcd(u_i - u_j, N), i \neq \mathrm{j}\}.$$

Make associated families

$\mathcal{S}(u_1\underline{g})$ $\mathcal{S}(u_2\underline{g})$ $\mathcal{S}(u_3\underline{g})$ … $\mathcal{S}(u_{p_{min}-1}\underline{g})$

Pick a sequence from each $\mathcal{S}(u_i\underline{g})$

An optimal family $\mathcal{F}(\underline{g})$ of N-ary perfect sequences of period N^2

Some interesting observation

Generators of **length p** (or odd N) over Z_p (or Z_N)	**Associate** polyphase sequences of **length p^2** (or odd N^2) over Z_p (or Z_N)
Hamming correlation properties	**Complex root-of-unity** correlation properties

Generator and their associated family

Generator perspective (Hamming correlation)		Sequences in associated families (correlation)
A generator $\underline{g}$ is an N-ary vector of length N	$\Leftrightarrow$	$\mathcal{S}(\underline{g})$ is a set of interleaved sequences $\mathcal{I}\left(\underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}\right)$ of length N^2

Generator and their associated family

Generator perspective (Hamming correlation)		Sequences in associated families (correlation)
A generator $\underline{g}$ is an N-ary vector of length N	$\Leftrightarrow$	$\mathcal{S}(\underline{g})$ is a set of interleaved sequences $\mathcal{I}\left(\underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}\right)$ of length N^2
$\underline{g}$ is a perfect generator iff Hamming correlation of $\underline{g}$ is perfect	$\Leftrightarrow$	Any member of $\mathcal{S}(\underline{g})$ is a perfect sequence

Generator and their associated family

Generator perspective (Hamming correlation)		Sequences in associated families (correlation)
A generator $\underline{g}$ is an N-ary vector of length N	$\Leftrightarrow$	$\mathcal{S}(\underline{g})$ is a set of interleaved sequences $\mathcal{I}\left(\underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m}\right)$ of length N^2
$\underline{g}$ is a perfect generator iff Hamming correlation of $\underline{g}$ is perfect	$\Leftrightarrow$	Any member of $\mathcal{S}(\underline{g})$ is a perfect sequence
$\underline{g}$ is an optimal generator iff Hamming correlation of $\underline{g}$ and $u\underline{g}$ is optimal for u and $u-1$ coprime to N	$\Leftrightarrow$	$\mathcal{S}(\underline{g})$ and $\mathcal{S}(u\underline{g})$ provide an optimal pair of perfect sequences for u and $u-1$ coprime to N

An **optimal generator** of length MK from an **optimal generator** of length K

- **Theorem.**
  Let $N = MK$ be an odd positive integer. If $\underline{h}$ is an optimal generator of length K, then the N-tuple $\underline{g}$ of size $M \times K$ given by

$$\mathcal{I}\left(\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \left(\underline{h} + K\underline{\alpha}\right)\right),$$

  is also an optimal generator, where
  - λ be a positive integer co-prime to N, and
  - $\underline{\alpha}$ be a K-tuple over $\mathbb{Z}_M$.

An **optimal generator** of length MK from an **optimal generator** of length K

- **Theorem.**
  Let $N = MK$ be an odd positive integer. If $\underline{h}$ is an optimal generator of length K, then the N-tuple $\underline{g}$ of size $M \times K$ given by

$$\mathcal{I}\left(\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \left(\underline{h} + K\underline{\alpha}\right)\right),$$

  is also an optimal generator, where
  - λ be a positive integer co-prime to N, and
  - $\underline{\alpha}$ be a K-tuple over $\mathbb{Z}_M$.

Recall that

we already have optimal generators of odd prime length!

Array form in detail

$$\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \left(\underline{\boldsymbol{h}} + K \underline{\alpha} \right)$$

Array form in detail

$$\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \left(\underline{\boldsymbol{h}} + K \underline{\alpha} \right)$$

$$= \lambda K \begin{bmatrix} 0 \\ 1 \\ \vdots \\ M-1 \end{bmatrix} \underbrace{[1, 1, \ldots, 1]}_{K \text{ times}} + \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \left(\underline{\boldsymbol{h}} + K \underline{\alpha} \right)$$

Proof can be found in the paper

example

- K=3, N=9, and $\underline{\boldsymbol{h}}$ = [0,1,2]
- $\lambda K \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} [1\ 1\ 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} (\underline{\boldsymbol{h}} + K\underline{\alpha})$

example

- K=3, N=9, and $\underline{\boldsymbol{h}}$ = [0,1,2]
- $\lambda K \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} [1\ 1\ 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} (\underline{\boldsymbol{h}} + K\underline{\alpha})$

$$= \lambda K \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} [1\ 1\ 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} ([0\ 1\ 2] + K\underline{\alpha})$$

example

- K=3, N=9, and $\underline{\boldsymbol{h}}$ = [0,1,2]

- $$\lambda K \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} [1\ 1\ 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} (\underline{\boldsymbol{h}} + K\underline{\alpha})$$

$$= \lambda K \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} [1\ 1\ 1] + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} ([0\ 1\ 2]\ + K\underline{\alpha})$$

$$= \lambda 3 \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{bmatrix} + \left(\begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} + \begin{bmatrix} 3\underline{\alpha} \\ 3\underline{\alpha} \\ 3\underline{\alpha} \end{bmatrix} \right)$$

example

- K=3, N=9, and $\underline{h}$ = [0,1,2]
- $\lambda K \begin{bmatrix}0\\1\\2\end{bmatrix}[1\ 1\ 1] + \begin{bmatrix}1\\1\\1\end{bmatrix}(\underline{h} + K\underline{\alpha})$

$$= \lambda K \begin{bmatrix}0\\1\\2\end{bmatrix}[1\ 1\ 1] + \begin{bmatrix}1\\1\\1\end{bmatrix}([0\ 1\ 2] + K\underline{\alpha})$$

$$= \lambda 3 \begin{bmatrix}0&0&0\\1&1&1\\2&2&2\end{bmatrix} + \left(\begin{bmatrix}0&1&2\\0&1&2\\0&1&2\end{bmatrix} + \begin{bmatrix}3\underline{\alpha}\\3\underline{\alpha}\\3\underline{\alpha}\end{bmatrix}\right)$$

- Use $\underline{\alpha}$ = [0 0 0] and $\lambda = 1$

$$= \begin{bmatrix}0&0&0\\3&3&3\\6&6&6\end{bmatrix} + \begin{bmatrix}0&1&2\\0&1&2\\0&1&2\end{bmatrix} = \begin{bmatrix}0&1&2\\3&4&5\\6&7&8\end{bmatrix}$$

example

- K=3, N=9, and $\underline{h}$ = [0,1,2]

- $\lambda K \begin{bmatrix}0\\1\\2\end{bmatrix}[1\ 1\ 1] + \begin{bmatrix}1\\1\\1\end{bmatrix}(\underline{h} + K\underline{\alpha})$

$$= \lambda K \begin{bmatrix}0\\1\\2\end{bmatrix}[1\ 1\ 1] + \begin{bmatrix}1\\1\\1\end{bmatrix}([0\ 1\ 2] + K\underline{\alpha})$$

$$= \lambda 3 \begin{bmatrix}0&0&0\\1&1&1\\2&2&2\end{bmatrix} + \left(\begin{bmatrix}0&1&2\\0&1&2\\0&1&2\end{bmatrix} + \begin{bmatrix}3\underline{\alpha}\\3\underline{\alpha}\\3\underline{\alpha}\end{bmatrix}\right)$$

- Use $\underline{\alpha}$ = [0 0 0] and $\lambda = 1$

$$= \begin{bmatrix}0&0&0\\3&3&3\\6&6&6\end{bmatrix} + \begin{bmatrix}0&1&2\\0&1&2\\0&1&2\end{bmatrix} = \begin{bmatrix}0&1&2\\3&4&5\\6&7&8\end{bmatrix}$$

- Finally, $\mathcal{I}\left(\begin{bmatrix}0&1&2\\3&4&5\\6&7&8\end{bmatrix}\right) = [0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8]$

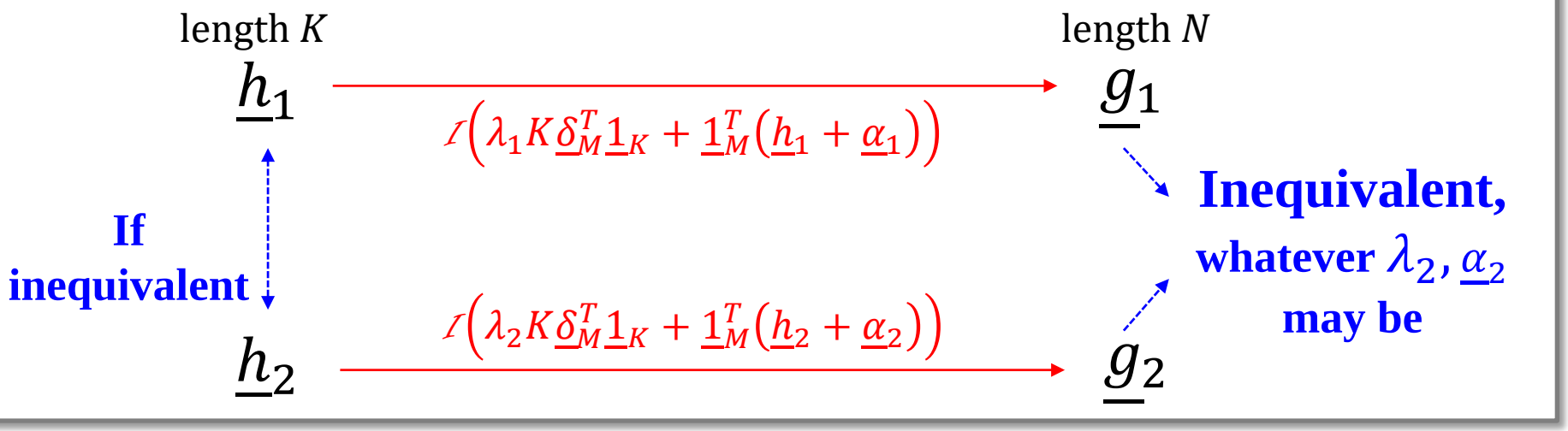
Example) $N = 9$ and $p = 3$

h	g	
$[0, 1, 2]$	$[0, 1, 2, 3, 4, 5, 6, 7, 8]$	← the original Frank sequence
	$[0, 1, 5, 3, 4, 8, 6, 7, 2]$	← New optimal generators
	$[0, 2, 1, 3, 5, 4, 6, 8, 7]$	
	$[0, 2, 4, 3, 5, 7, 6, 8, 1]$	

3 new optimal generators!

Some equivalence

Input perspective



Some equivalence

Input perspective

length K $\underline{h}_1$ $\xrightarrow{\mathcal{I}\left(\lambda_1 K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(\underline{h}_1 + \underline{\alpha}_1)\right)}$ length N $\underline{g}_1$

$\underline{h}_2$ $\xrightarrow{\mathcal{I}\left(\lambda_2 K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(\underline{h}_2 + \underline{\alpha}_2)\right)}$ $\underline{g}_2$

If inequivalent

Inequivalent, whatever λ_2, $\underline{\alpha}_2$ may be

Output perspective

$\underline{h}_1$ $\xrightarrow{\mathcal{I}\left(\lambda_1 K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T(\underline{h}_1 + \underline{\alpha}_1)\right)}$ $\underline{g}_1$

If Equivalent

Can find $\underline{h}_2$ for $\underline{g}_2$

$\underline{h}_2$ $\leftarrow$ $\underline{g}_2$

Equivalent to $\underline{h}_1$

Optimal family construction

A given optimal generator $\underline{g}$ of odd length N

$$\mathcal{U} = \{u_i \,|\, \gcd(u_i, N) = 1 = \gcd(u_i - u_j, N), i \neq \mathrm{j}\}.$$

Make associated families

$\mathcal{S}(u_1\underline{g})$ $\mathcal{S}(u_2\underline{g})$ $\mathcal{S}(u_3\underline{g})$ … $\mathcal{S}(u_{p_{min}-1}\underline{g})$

Pick a sequence from each $\mathcal{S}(u_i\underline{g})$

An optimal family $\mathcal{F}(\underline{g})$ of N-ary perfect sequences of period N^2

Example) $N = 15$ and $p = 3, 5$

h	g
$[0,1,2,3,4]$	$[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14]$ ← the original Frank sequence
	$[0,1,2,3,9,5,6,7,8,14,10,11,12,13,4]$
	$[0,1,2,8,9,5,6,7,13,14,10,11,12,3,4]$
	$[0,1,2,8,14,5,6,7,13,4,10,11,12,3,9]$
	$[0,1,7,8,4,5,6,12,13,9,10,11,2,3,14]$
	$[0,1,7,8,9,5,6,12,13,14,10,11,2,3,4]$
	$[0,1,7,8,14,5,6,12,13,4,10,11,2,3,9]$
	$[0,1,7,13,4,5,6,12,3,9,10,11,2,8,14]$
	$[0,1,7,13,9,5,6,12,3,14,10,11,2,8,4]$
	$[0,1,7,13,14,5,6,12,3,4,10,11,2,8,9]$
	$[0,6,7,8,9,5,11,12,13,14,10,1,2,3,4]$
	$[0,6,7,8,14,5,11,12,13,4,10,1,2,3,9]$
	$[0,6,7,13,14,5,11,12,3,4,10,1,2,8,9]$
	$[0,6,12,13,9,5,11,2,3,14,10,1,7,8,4]$
$[0,1,3,2,4]$	$[0,1,3,2,4,5,6,8,7,9,10,11,13,12,14]$
	$[0,1,3,2,9,5,6,8,7,14,10,11,13,12,4]$
	$[0,1,3,2,14,5,6,8,7,4,10,11,13,12,9]$
	$[0,1,3,7,4,5,6,8,12,9,10,11,13,2,14]$
	$[0,1,3,7,9,5,6,8,12,14,10,11,13,2,4]$
	$[0,1,3,7,14,5,6,8,12,4,10,11,13,2,9]$
	$[0,1,3,12,4,5,6,8,2,9,10,11,13,7,14]$
	$[0,1,3,12,9,5,6,8,2,14,10,11,13,7,4]$
	$[0,1,3,12,14,5,6,8,2,4,10,11,13,7,9]$
	$[0,1,8,12,4,5,6,13,2,9,10,11,3,7,14]$
	$[0,6,3,2,9,5,11,8,7,14,10,1,13,12,4]$
	$[0,6,3,2,14,5,11,8,7,4,10,1,13,12,9]$
	$[0,6,3,7,9,5,11,8,12,14,10,1,13,2,4]$
	$[0,6,13,2,9,5,11,3,7,14,10,1,8,12,4]$

← 27 New optimal generators

h	g
$[0,1,2]$	$[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14]$
	$[0,1,5,3,4,8,6,7,11,9,10,14,12,13,2]$
	$[0,4,5,3,7,8,6,10,11,9,13,14,12,1,2]$
	$[0,4,8,3,7,11,6,10,14,9,13,2,12,1,5]$
	$[0,4,14,3,7,2,6,10,5,9,13,8,12,1,11]$

4 New optimal generators

31 new optimal generators!

Interesting questions (concluding)

1. For an odd N, find the **maximum number of inequivalent** optimal generators of length N.

Interesting questions (concluding)

1. For an odd N, find the **maximum number of inequivalent** optimal generators of length N.

2. Consider a positive odd integer N, which has two distinct prime factors, i.e.,

$$N = p_1 M_1 = p_2 M_2.$$

What is **the relationship** between two optimal generators of length N which come from optimal generators of length p_1 and p_2 respectively?

Interesting questions (concluding)

1. For an odd N, find the **maximum number of inequivalent** optimal generators of length N.

2. Consider a positive odd integer N, which has two distinct prime factors, i.e.,
$$N = p_1 M_1 = p_2 M_2.$$
What is **the relationship** between two optimal generators of length N which come from optimal generators of length p_1 and p_2 respectively?

3. Can we obtain all the optimal generators of odd length N by using the proposed construction? If not, how can we get them?