A construction of optimal generators of odd lengths for perfect sequence families

CSDL

Min Kyu Song, Gangsan Kim, and Hong-Yeop Song

Yonsei University

IWSDA 2017, October 24-28

Notation

- p : an odd prime
- N : a positive integer (usually a composite number)
- $\mathbb{Z}$: the set of integers
- $\mathbb{Z}_N$: the integers modulo N
- $\underline{0}_N$: the all-zero vector of length N
- $\underline{1}_N$: the all-one vector of length N
- $\underline{\delta}_N$: the vector of the form $[0,1,2, \dots, N-1]$

Correlation

- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{N^2-1}$ and $\boldsymbol{y} = \{y(n)\}_{n=0}^{N^2-1}$ be two N-ary sequences of length N^2, then (periodic) correlation between $\boldsymbol{x}$ and $\boldsymbol{y}$ at time shift τ is

$$\mathrm{C}_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{n=0}^{N^2-1} \omega_N^{x(n)-y(n+\tau)}$$

where $\omega_N = e^{-\frac{j2\pi}{N}}$.

  - A sequence is referred to a **perfect sequence** if its autocorrelation is zero for any time shift $\tau \not\equiv 0 \ (mod\ N^2)$.

The Sarwate bound

- Cross correlation of any two perfect sequences of length N^2 is greater than or equal to N.
- A set of perfect sequences is called optimal when the equality holds for cross-correlation of any two distinct sequences in the set.

Hamming correlation

- For some purpose, we also consider the Hamming correlation.

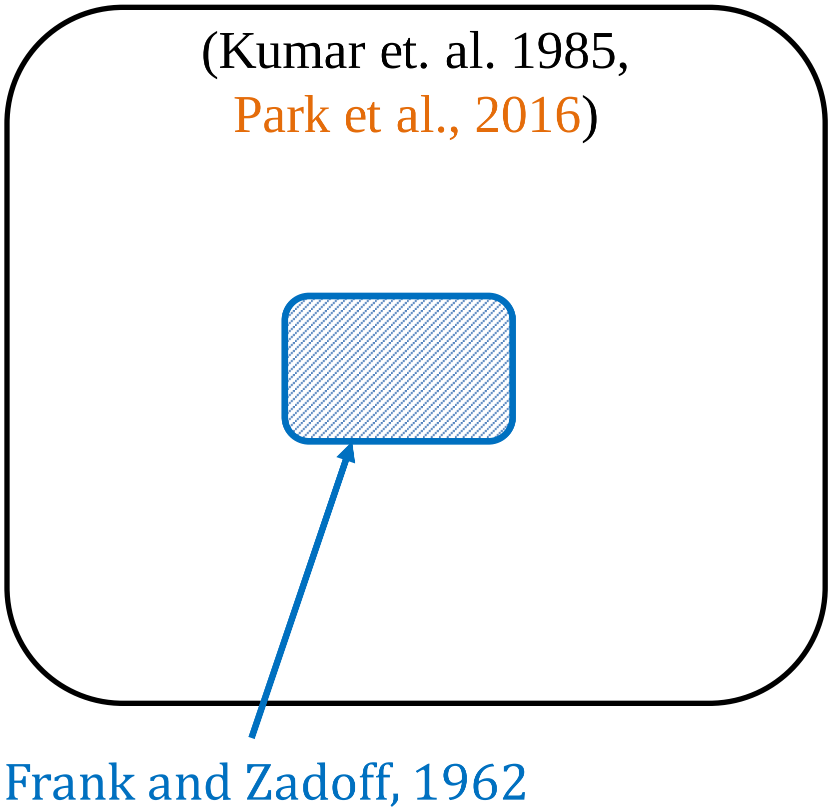
- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{L-1}$ and $\boldsymbol{y} = \{y(n)\}_{n=0}^{L-1}$ be two sequences of length L over $\mathbb{Z}_M$, the Hamming correlation between $\boldsymbol{x}$ and $\boldsymbol{y}$ at time shift τ, denoted by $\mathrm{H}_{\boldsymbol{x},\boldsymbol{y}}(\tau)$, is given by

$$\mathrm{H}_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{n=0}^{L-1} \mathrm{h}(x(n), y(n+\tau)),$$

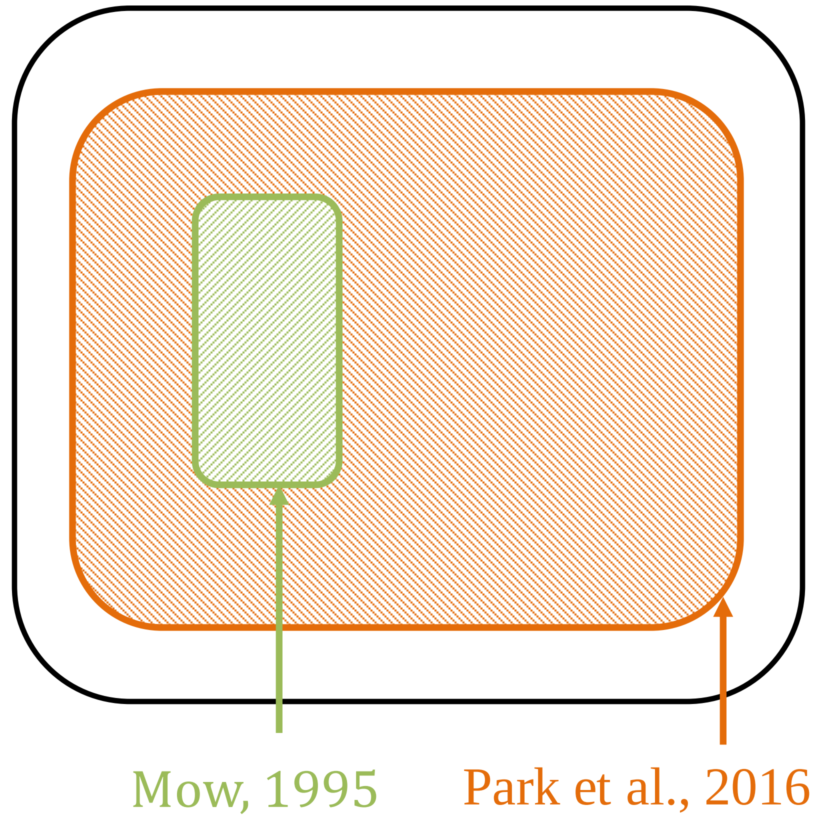
where $\mathrm{h}(a,b) = \begin{cases} 1, & \text{if } a \equiv b \pmod{M} \\ 0, & \text{otherwise} \end{cases}$

Case : p-ary, p^2 period

p-ary perfect sequences of period p^2

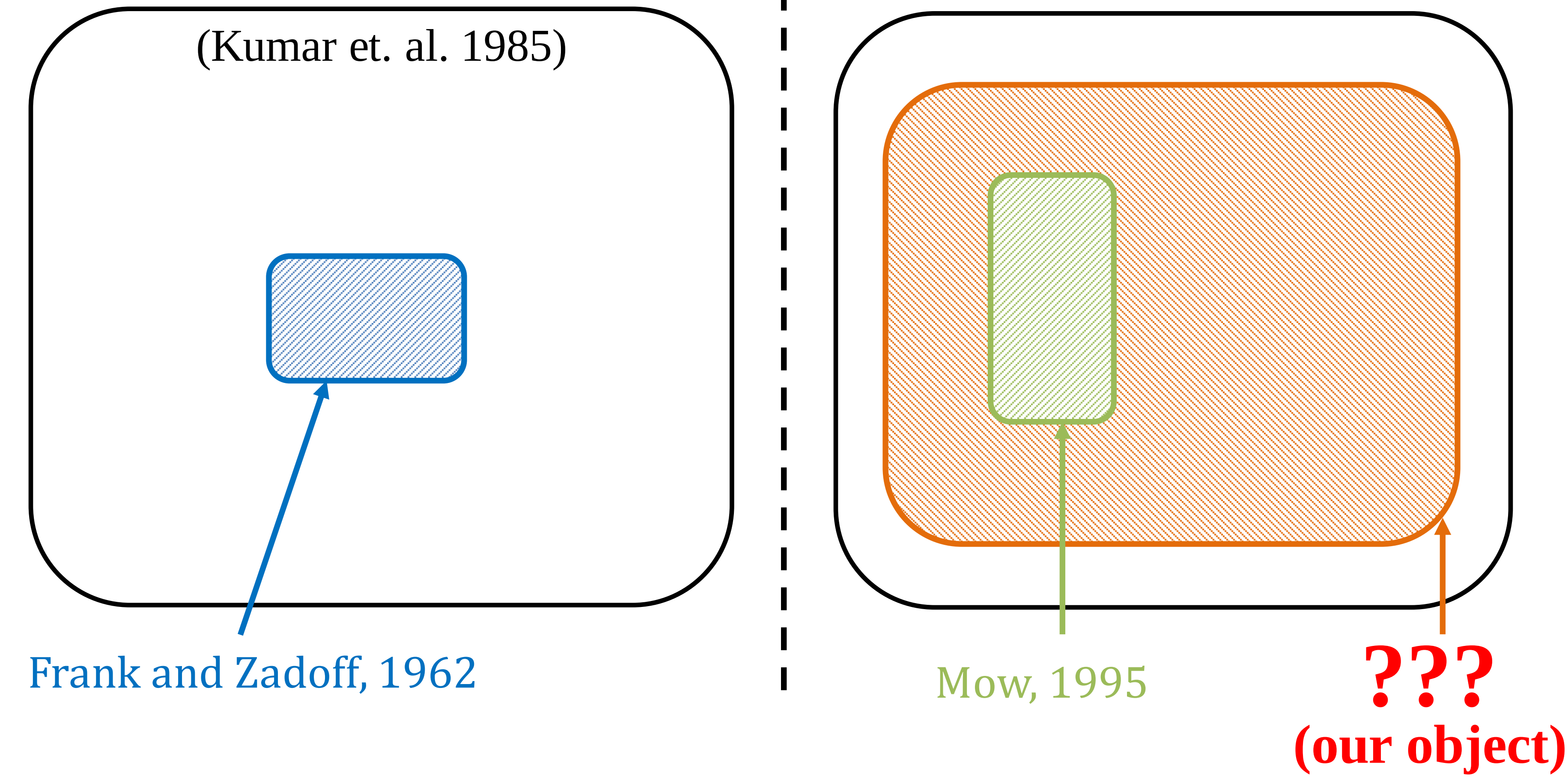


optimal sets of p-ary perfect sequences of period p^2



Case : N-ary, N^2 period

N-ary perfect sequences of period N^2 | optimal sets of N-ary perfect sequences of period N^2



Interesting structure

array form

$$\mathbf{X} = \underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m} \ \ (mod\ N)$$

$$= \begin{bmatrix} 0 \\ 1 \\ \vdots \\ N-1 \end{bmatrix} \underline{g} + \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \underline{m} \ \ (\text{mod } N)$$

$$= \begin{bmatrix} \underline{0} + \underline{m} \\ \underline{g} + \underline{m} \\ \vdots \\ (N-1)\underline{g} + \underline{m} \end{bmatrix} \ (\text{mod } N)$$

sequence

$$\boldsymbol{x} = \left[\underline{0} + \underline{m}, \underline{g} + \underline{m}, 2\underline{g} + \underline{m}, \cdots, (N-1)\underline{g} + \underline{m}\right] \ \ (\text{mod } N)$$

Generators and associated families

- For an array given by

$$\mathbf{X} = \underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m} \pmod{N},$$

  - 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 $\mathcal{S}(\underline{g})$.
  - Note that there are N^N different choice of $\underline{m}$ over $\mathbb{Z}_N$.

- A fact is that, there exists some $\underline{g}$ such that all the sequences in its associated family are perfect.

Perfect generators

- 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.

- Theorem. (Necessary and sufficient condition)
  A generator $\underline{g}$ of length N is a perfect generator if and only if every element of $\mathbb{Z}_N$ appears once.

- Corollary.
  If a generator $\underline{g}$ is perfect, then, for any integer u co-prime to N, $u\underline{g}$ is also a perfect generator.

For the Hamming correlation perspective …

- Every element of $\mathbb{Z}_N$ appears once in $\underline{g}$

  $\Leftrightarrow$ Every perfect generator has

$$\mathrm{H}_{\underline{g}}(\tau) = \begin{cases} N, & \text{if } \tau \equiv 0 \pmod{N} \\ 0, & \text{otherwise} \end{cases}$$

  as its Hamming autocorrelation profile.

Optimal generators

- Definition. (Optimal generators)
  A generator $\underline{g}$ of length N is an optimal generator if it is a perfect generator and any two sequences of period N^2 in $S(u\underline{g}), S(v\underline{g})$ have N as their correlation magnitude for any non-zero integers u, v which are co-prime to N with

$$\gcd(u - v, N) = 1.$$

- That is, for such integers u, v, the Hamming correlation of $u\underline{g}$ and $v\underline{g}$ is always one regardless of τ.

- If N is even, there is no such u, v pair (all u, v, and $u - v$ are co-prime to N.) So, all the optimal generators are odd lengths.

Necessary and sufficient condition on optimal generators

- Theorem.
  A generator $\underline{g}$ of length N is an optimal generator
  if and only if
  $$\mathrm{H}_{u\underline{g},v\underline{g}}(\tau) = 1,$$
  for any τ and any two integers $u \not\equiv v \ (mod\ N)$ such that all of u, v, and $u - v$ are co-prime to N.

Optimal generators and one-coincidence sequences

- The problem "Finding an optimal family of N-ary perfect sequences of period N^2" is changed to "finding a set of hopping sequences of length N with N hopping slots with following Hamming correlation profile"
  1. Non-trivial Hamming autocorrelation is zero for any sequence.
  2. Hamming crosscorrelation of any two sequences of length N in the set is one.

- Such a set of hopping sequences is a special class of one-coincidence sequences.

How to use optimal

- For a given optimal generator $\underline{g}$ of odd length N, an optimal family $\mathcal{F}(\underline{g})$ of perfect sequences of period N^2 can be constructed by

$$\mathcal{F}(\underline{g}) = \left\{ \boldsymbol{f}_i \in \mathcal{S}(u_i\underline{g}) \middle| u_i \in \mathcal{U} \right\}$$

where

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

- There are $p_{\min} - 1$ sequences in $\mathcal{F}(\underline{g})$, where $p_{\min}$ is the smallest prime factor of N. e.g., $\mathcal{U} = \{1, 2, \ldots, p_{\min} - 1\}$.

Optimal family construction process

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

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

Make associated families

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

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

A recursive construction for optimal generators

- Theorem.
  Let $N = MK$ be an odd positive integer, and λ be a positive integer co-prime to N.
  If $\underline{h}$ is an optimal generator of length K,
  then the N-tuple $\underline{g}$, whose array $\boldsymbol{G}$ of size $M \times K$ is given by

$$\boldsymbol{G} = \lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \underline{h} \pmod N,$$

  is also an optimal generator.

- Since Park et al. proposed $\phi(p)$ optimal generators of length p, by using them as inputs of our recursive construction, we can get any odd length

Proof

- We first show that $\underline{g}$ is a perfect generator by observing that

$$\boldsymbol{G} = \lambda K \begin{bmatrix} 0 \\ 1 \\ \vdots \\ M-1 \end{bmatrix} \underbrace{[1, 1, 1, \dots, 1]}_{K \text{ times}} + \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \underline{h}$$

$$= \lambda \begin{bmatrix} 0 & 0 & \cdots & 0 \\ K & K & \cdots & K \\ \vdots & \vdots & \ddots & \vdots \\ (M-1)K & (M-1)K & \cdots & (M-1)K \end{bmatrix} + \begin{bmatrix} \underline{h} \\ \underline{h} \\ \vdots \\ \underline{h} \end{bmatrix}.$$

Proof (cont')

- $\underline{g}$ is an optimal generator

  $\Leftrightarrow u\underline{g} - v\mathcal{T}_\tau(\underline{g}) \pmod N$ has only one zero for any u, v

  such that $u, v, u - v$ are co-prime to N.

  1) when $\tau \equiv 0 \pmod N$ is obvious.

$$u\underline{g} - v\underline{g} = (u - v)\underline{g}$$

co-prime to N Has only one zero

(Since it is perfect)

Proof (cont')

2) when $\tau \not\equiv 0 \pmod{N}$, let $\tau = qK + r$ with $0 \le r < K$ and consider the array form of $\mathcal{T}_\tau(\underline{g})$, denoted by $\mathcal{T}_\tau(\boldsymbol{G})$.

$$\mathcal{T}_\tau(\boldsymbol{G}) = \mathcal{T}_\tau(\lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \underline{h})$$

$$= \lambda K\, \mathcal{T}_\tau(\underline{\delta}_M^T \underline{1}_K) + \mathcal{T}_\tau(\underline{1}_M^T \underline{h})$$

$$\mathcal{T}_\tau(\underline{1}_M^T \underline{h}) = \underline{1}_M^T \mathcal{T}_\tau(\underline{h})$$

$$\mathcal{T}_\tau(\underline{\delta}_M^T \underline{1}_K) = \lambda K \begin{bmatrix} q\underline{1}_{M-r} & (q+1)\underline{1}_r \\ (q+1)\underline{1}_{M-r} & (q+2)\underline{1}_r \\ \vdots & \vdots \\ \underline{0}_{M-r} & \underline{1}_r \end{bmatrix}$$

$$= \lambda K \underline{1}_K^T [q\underline{1}_{N-r} \quad (q+1)\underline{1}_r] + \lambda K \underline{\delta}_M^T \underline{1}_K$$

Proof (cont')

So,

$$\mathcal{T}_\tau(\boldsymbol{G}) = \lambda K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \mathcal{T}_\tau\left(\underline{h}\right) + \lambda K \underline{1}_M^T \underline{m}$$

where $\underline{m} = [q\underline{1}_{N-r} \quad (q+1)\underline{1}_r]$.

Finally, we get

$$\begin{aligned} & u\boldsymbol{G} - v\mathcal{T}_\tau(\boldsymbol{G}) \\ & = u\lambda K \underline{\delta}_M^T \underline{1}_K + u\underline{1}_M^T \underline{h} \\ & \quad -v\lambda K \underline{\delta}_M^T \underline{1}_K - v\underline{1}_M^T \mathcal{T}_\tau\left(\underline{h}\right) - v\lambda K \underline{1}_M^T \underline{m} \\ & = (u-v)\lambda K \underline{\delta}_M^T \underline{1}_K + \left(u\underline{h} - v\mathcal{T}_\tau\left(\underline{h}\right)\right) - v\lambda K \underline{1}_M^T \underline{m} \\ & = (u-v) K \underline{\delta}_M^T \underline{1}_K + \underline{1}_M^T \left(u\underline{h} - v\mathcal{T}_\tau\left(\underline{h}\right)\right) - v\lambda K \underline{1}_M^T \underline{m} \end{aligned}$$

Proof (cont')

$$uG - v\mathcal{T}_\tau(G)$$

$$= (u-v)K\underline{\delta}_M^T\underline{1}_K + \underline{1}_M^T\left(u\underline{h} - v\mathcal{T}_\tau(\underline{h})\right) - v\lambda K\underline{1}_M^T\underline{m}$$

All the rows are the same.
Every row has only one element which is congruent to 0 modulo K.

All the columns are the same.
Each column has the following properties:

1. All the terms are multiples of K and are not congruent to each other over $\mathbb{Z}_N$.
2. The very first element is congruent to 0 modulo $N = MK$.

This term just works as a bias of each column. Each column bias is a multiple of K.

Therefore, we finally conclude that $uG - v\mathcal{T}_\tau(G)$ has **only one element congruent to 0 modulo N.**

Equivalence

- Definition.
  For given two generators (or sequences) of the same length, we say that they are equivalent if we can obtain one from another by applying constant multiples, cyclic shifts, and decimations.

- Corollary.
  Let $\underline{g}$ and $\underline{f}$ be two perfect generators of length N.
  If $\underline{g}$ and $\underline{f}$ are inequivalent, then any two N-ary perfect sequences of period N^2 from $\mathcal{S}(\underline{g})$ and $\mathcal{S}(\underline{f})$, respectively, also does.

Array form of decimated sequence

- Lemma.
  Let x be a sequence whose array form is given by

$$\mathbf{X} = \underline{\delta}_N^T \underline{g} + \underline{1}_N^T \underline{m} \pmod{N}.$$

The array form of d-decimation of a sequence $\boldsymbol{x}$, denoted by $D_d(\boldsymbol{X})$, is

$$D_d(\boldsymbol{X}) = d\underline{\delta}_N^T D_d(\underline{g}) + \underline{1}_N^T \underline{m}''(mod\ N)$$

where

$$\underline{m}'' = D_d(\underline{m}) + \left[0, \left\lfloor \frac{d}{N} \right\rfloor, \left\lfloor \frac{2d}{N} \right\rfloor, \cdots, \left\lfloor \frac{d(N-1)}{N} \right\rfloor\right].$$

Comparison to previous

- Mow's construction gives a set of decimated Frank sequences of period N^2.
  Since d-decimation of the generator of the original Frank sequence is

$$[0, 1, 2, \ldots, N-1],$$

  his construction is exactly same to our construction with the above generator.

Example

Two inequivalent optimal generators of length 5

$h_1 = [0, 1, 2, 3, 4]$ $\qquad$ $h_2 = [0, 1, 3, 2, 4]$

$M = 3, \lambda = 1$

$\underline{g}_1 = [0, 1, 2, 3, \ldots, 14]$ $\qquad$ $g_2 = [0, 1, 3, 2, 4, 5, 6, 8, 7, 9, 10, 11, 13, 12, 14]$

Two inequivalent optimal generators of length 15

Some interesting questions

1. For a given positive odd integer N and its largest prime factor $p_{\max}$, we know that there always exists $\phi(p_{\max})$ optimal generators.
   What is the exact number of 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?