## Recent development on perfect polyphase sequences and optimal families

Min Kyu Song and Hong-Yeop Song Yonsei University

2018 Information Theory and Applications Workshop Feb. 11-16, 2018 Catamaran Resort, San Diego, USA

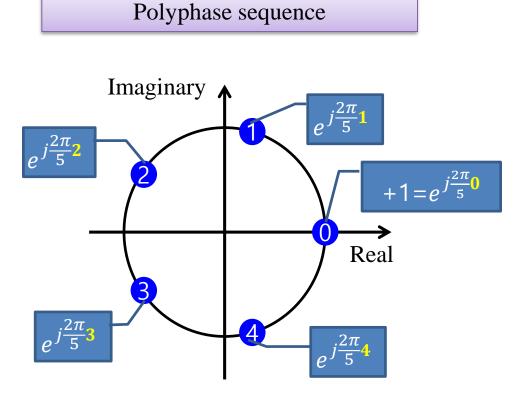


#### In this talk...

- 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 sets of N-ary perfect polyphase sequences of period  $N^2$  with respect to Sarwate bound

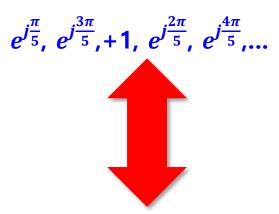


#### **Polyphase sequences**



Polyphase sequence representation

Complex valued sequence



• Phase sequence over the integers **modulo 5** 

1, 3, 0, 2, 4, ...

⇒ It can be equivalently described by its phase sequence



#### Correlation

Let x = {x(n)}<sup>L-1</sup><sub>n=0</sub> and y = {y(n)}<sup>L-1</sup><sub>n=0</sub> be two N-ary sequences of length L, then (periodic) correlation between x and y at time shift τ is

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

where 
$$\omega_N = e^{-j\frac{2\pi}{N}}$$

- It is called autocorrelation if y is a cyclic-shifted version of x.
- It is called **crosscorrelation** otherwise.
- A sequence is referred to a '*perfect sequence*' if its autocorrelation is zero for any shift τ ≠ 0 (mod L).



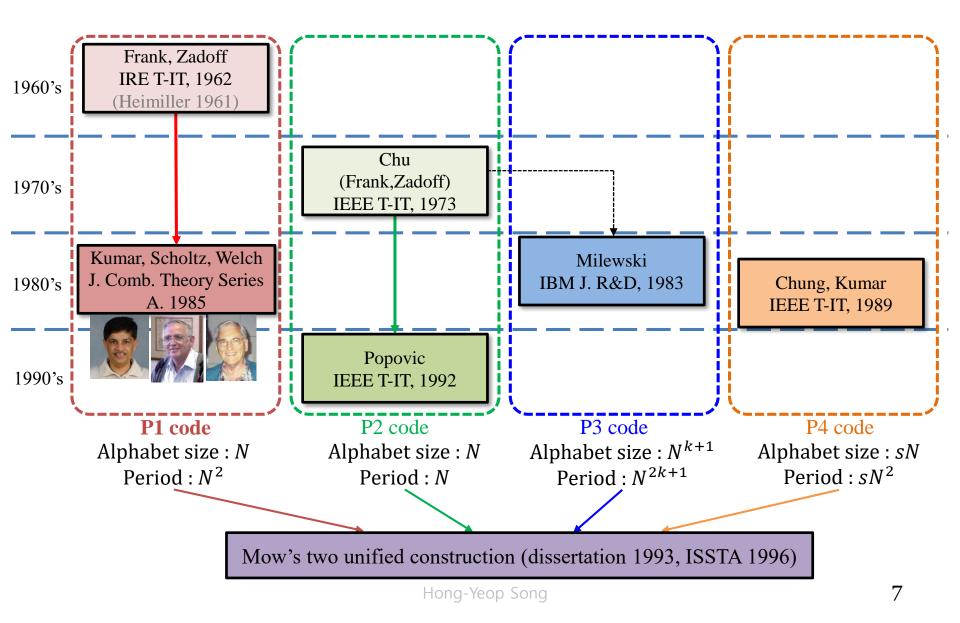
#### Sarwate bound

- 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.

Earlier...

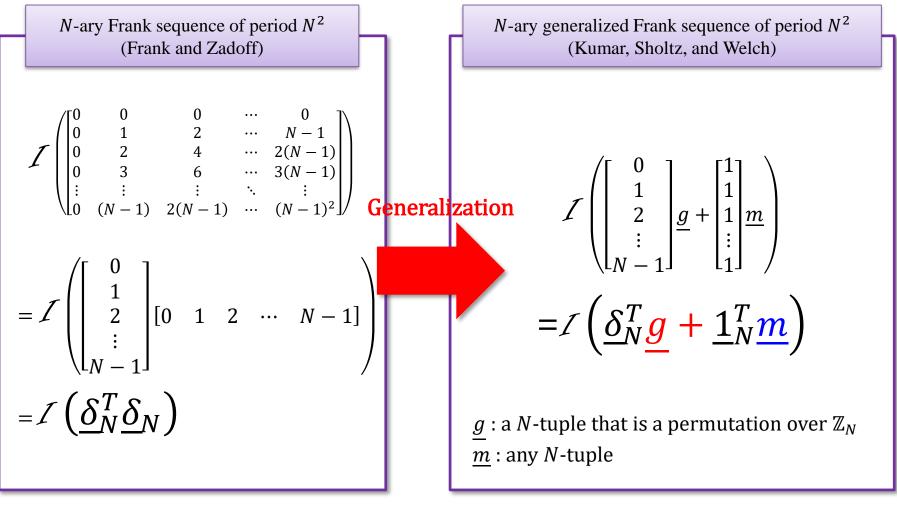


# History of constructing perfect polyphase sequences





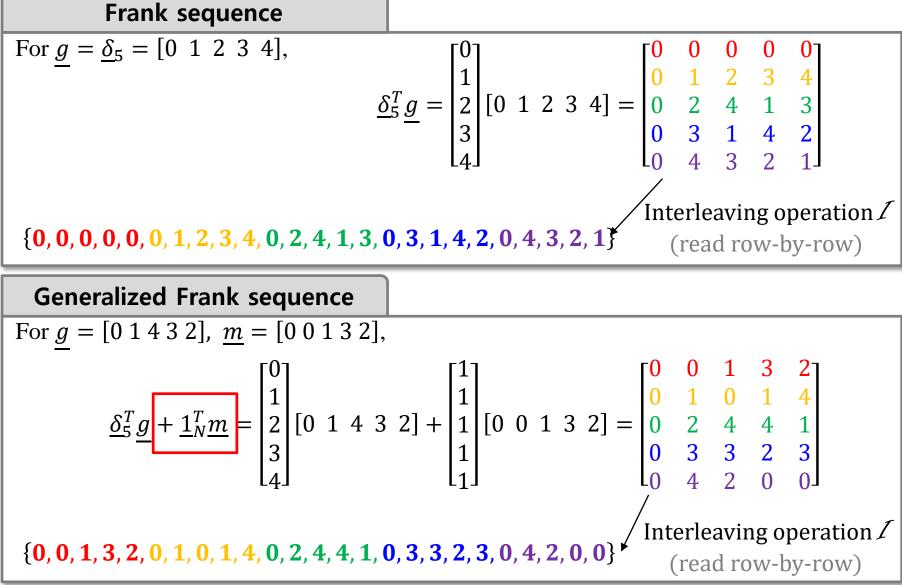
#### P1 codes



Where  $\mathcal{I}(X)$  stands for the operation that generates a sequences by reading X row-by-row,  $\underline{\delta}_N \triangleq \begin{bmatrix} 0 & 1 & 2 & \cdots & N-1 \end{bmatrix}$ , and  $\underline{1}_N = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$ Hong-Yeop Song N times 8

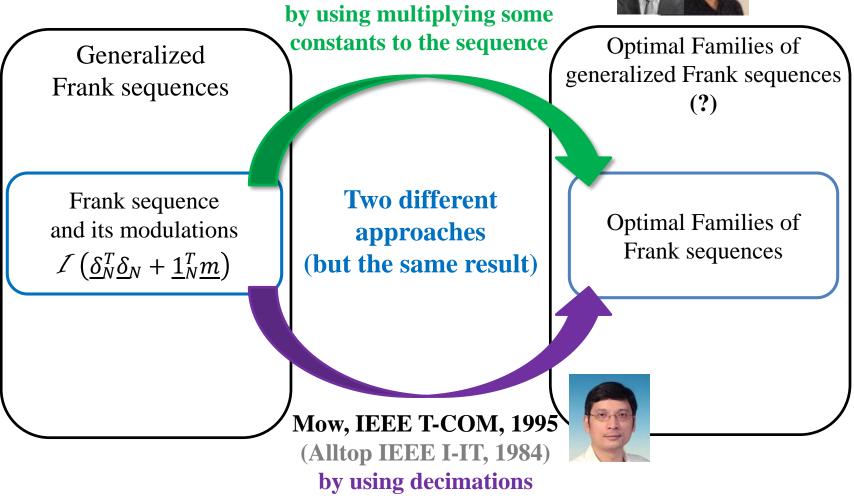


#### **Example** (*N* = 5)



#### Constructing optimal Families from P1 codes





Hong-Yeop Song

## **Brief review of two constructions**

#### Suehiro and Hatori 1988

 $\mathcal{U} \triangleq \{u_i \in \mathbb{Z}_N | \gcd(u_i, N) = 1, u_i \not\equiv u_i \text{ if } i \neq j, \gcd(u_i - u_i, N) = 1\}$  $\underline{m}_1, \underline{m}_2, \dots, \underline{m}_{|\mathcal{U}|}$  : **arbitrary** chosen *N*-tuples. Optimal family  $S = \left\{ \mathcal{I}\left(\underline{\delta}_{N}^{T} u_{i} \underline{\delta}_{N} + \underline{1}_{N}^{T} \underline{m}_{i}\right) | u_{i} \in \mathcal{U} \right\}$ **Modulatable sequences** (named by Suehiro and Hatori) Mow 1995 (Alltop 1984, N prime)  $\mathcal{U} \triangleq \left\{ u_i \in \mathbb{Z}_N \middle| \gcd(u_i, N) = 1, u_i \not\equiv u_i \text{ if } i \neq j, \gcd(u_i - u_i, N) = 1 \right\}$  $\underline{m}_1, \underline{m}_2, \dots, \underline{m}_{|\mathcal{U}|}$  : **arbitrary** chosen *N*-tuples. Optimal family  $S = \left\{ \mathfrak{D}_d \left( \mathcal{I} \left( \underline{\delta}_N^T \underline{\delta}_N + \underline{1}_N^T \underline{m}_i \right) \right) \middle| d \in \mathcal{U} \right\}$ 

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

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

#### • Theorem.

For any odd prime p, the p-ary Fermat-quotient sequence 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) 
$$\boldsymbol{q} \Leftrightarrow \begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 0 & 4 & 0 & 4 & 2 \\ 0 & 3 & 2 & 2 & 3 \\ 0 & 2 & 4 & 0 & 4 \\ 0 & 1 & 1 & 3 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} \begin{bmatrix} 0, 4, 2, 3, 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0, 0, 3, 1, 1 \end{bmatrix}$$

- Therefore, it is a subclass of the generalized Frank sequences.
- We call *g* a generator.
- We call a collection of all the possible sequences for a fixed <u>g</u> an associated family of <u>g</u> and denote it by S(<u>g</u>). That is, S(<u>g</u>) is the set of all the modulations of I(<u>S</u><sup>T</sup><sub>p</sub><u>g</u>)



#### In general...

- Definition. (Perfect generators)
   A generator <u>g</u> is a perfect generator
   if all the sequences s ∈ S(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.

- b) *g* is perfect generator.
- 2) *g* is a permutation of  $\mathbb{Z}_p$ .

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



#### **Transformations**

#### • Definition.

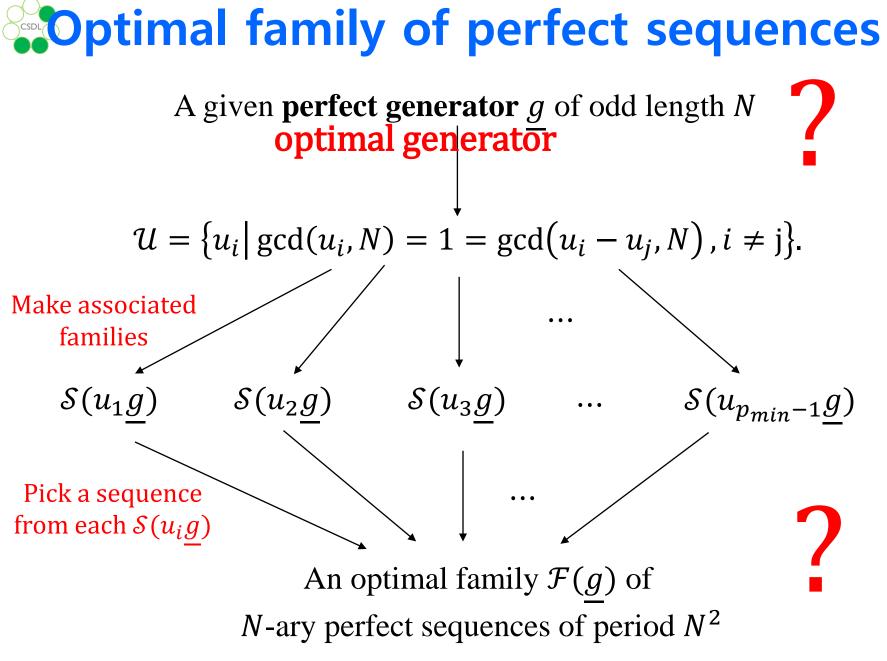
Let g be a generator of length p.

- 1) (cyclic shifts) Shifting g cyclically to the left by  $\tau$ .
- 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  $d \neq 0 \pmod{p}$ .
- With an abuse, we use these transformations for sequences.

#### Corollary.

Let 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 generators**

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

- Theorem. For an odd prime p, let <u>g</u><sub>m,τ,κ</sub> be a p-tuple over Z<sub>p</sub> where its n-th term, denoted by g(n; m, τ, κ), is given by g(n; m, τ, κ) ≡ m(n + τ)<sup>κ</sup> (mod p)
  where κ is an integer coprime to p - 1, m ≠ 0 (mod p), and τ is an integer. Then, <u>g</u> is an optimal generator of length p.
- Two optimal generators  $\underline{g}_{m,\tau,\kappa}$  and  $\underline{g}_{m,\mu,\lambda}$  are equivalent if and only if  $\kappa \equiv \lambda \pmod{p-1}$ .
- Therefore, we have  $\phi(p-1)$  inequivalent optimal generators.

# Inequivalent optimal generators

p	optimal generators (representatives)	$\kappa$
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} <b>(FQ)</b>	5
	$\{0,1,2,3,4,5,6,7,8,9,10\}$ (Frank)	1
11	$\{0,1,6,4,3,9,2,8,7,5,10\}$ (FQ)	9
11	{0,1,7,9,5,3,8,6,2,4,10}	7
	{0,1,8,5,9,4,7,2,6,3,10}	3
	$\{0,1,2,3,4,5,6,7,8,9,10,11,12\}$ (Frank)	1
13	{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* (recently accepted)

# Perfect generators of any length

• We now extend the previous results by considering  $\mathcal{I}\left(\underline{\delta}_{N}^{T}g + \underline{1}_{N}^{T}\underline{m}\right),$ 

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

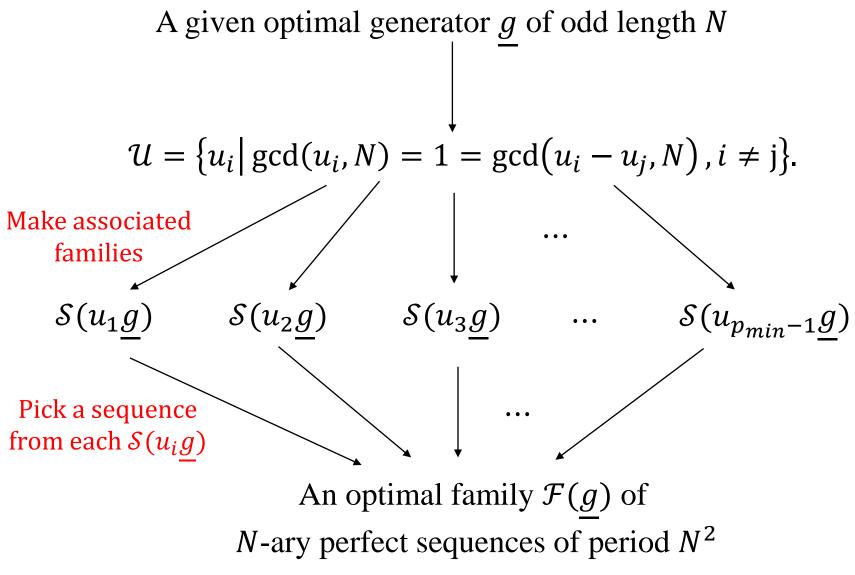
- Definition. (Perfect generators)
   A generator <u>g</u> of length N is a perfect generator
   if any sequence in its associated family S(g) is perfect.
- Obviously, a generator of any *N*-ary generalized Frank sequences of period  $N^2$  is a perfect generator.

# Optimal generators of odd length

Definition. (optimal generators of odd lengths) A generator <u>g</u> is a optimal generator if any pair of x ∈ S(<u>g</u>) and y ∈ S(u<u>g</u>) 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**



Hong-Yeop Song

#### Generator and their associated family

**Generator perspective** (Hamming correlation)

Sequences in associated families (correlation)

A generator <u>g</u> is an *N*-ary vector of length *N*   $S(\underline{g})$  is a set of interleaved sequences  $I(\underline{\delta}_{N}^{T}\underline{g} + \underline{1}_{N}^{T}\underline{m})$  of length  $N^{2}$ 

 $\underline{g}$  is a perfect generator iff Hamming correlation of g is perfect

 $\Leftrightarrow$ 

Any member of  $S(\underline{g})$  is a perfect sequence

<u>*g*</u> is an optimal generator iff Hamming correlation of <u>*g*</u> and <u>*ug*</u> is optimal for *u* and u - 1 coprime to *N*   $S(\underline{g})$  and  $S(u\underline{g})$  provide an optimal pair of perfect sequences for u and u - 1 coprime to N



#### **A recursive construction**

• Theorem. (a recursive construction) Let N = MK be an odd positive integer. If <u>h</u> is an optimal generator of length *K*, then the *N*-tuple <u>g</u> of size  $M \times K$  given by

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

is also an optimal generator, where

- $\lambda$  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!

Hong-Yeop Song



#### **Array form**

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

#### Proof can be found in the paper



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

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

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



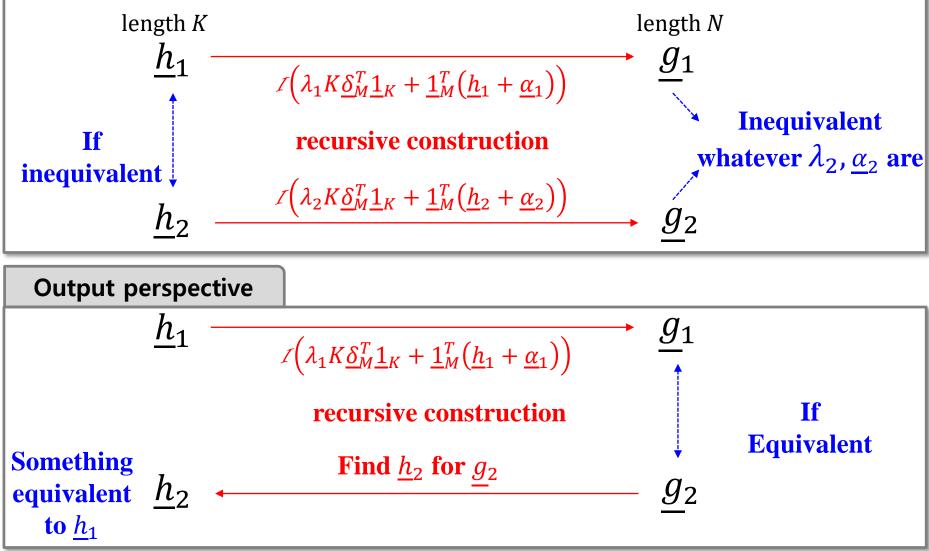
#### Example) N = 9 and p = 3

#### **3 new optimal generators!**

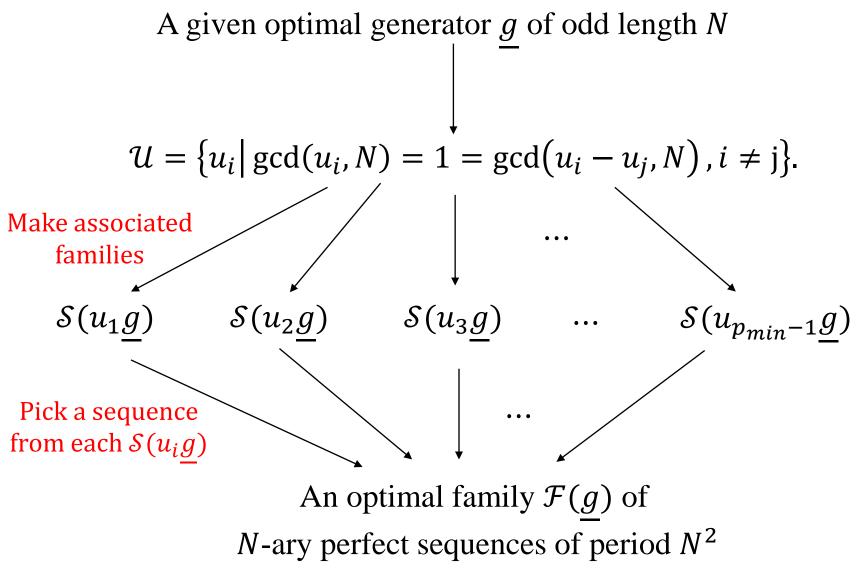


#### Some equivalence

#### Input perspective



### **Optimal family construction**



Hong-Yeop Song



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

$\underline{h}$	<u>g</u>			
	$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14] \leftarrow$	- the orig	ginal Fra	nk sequence ———
[0, 1, 2, 3, 4]	[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]		Ь	
	[0, 1, 7, 8, 4, 5, 6, 12, 13, 9, 10, 11, 2, 3, 14]		$\underline{h}$	<u> </u>
	[0, 1, 7, 8, 9, 5, 6, 12, 13, 14, 10, 11, 2, 3, 4]			[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]
	[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, 5, 3, 4, 8, 6, 7, 11, 9, 10, 14, 12, 13, 2]
	[0, 1, 7, 13, 9, 5, 6, 12, 3, 14, 10, 11, 2, 8, 4]		[0, 1, 2]	[0, 4, 5, 3, 7, 8, 6, 10, 11, 9, 13, 14, 12, 1, 2]
	[0, 1, 7, 13, 14, 5, 6, 12, 3, 4, 10, 11, 2, 8, 9]			
	$\begin{bmatrix} 0, 6, 7, 8, 9, 5, 11, 12, 13, 14, 10, 1, 2, 3, 4 \end{bmatrix}$ $\begin{bmatrix} 0, 6, 7, 8, 14, 5, 11, 12, 13, 4, 10, 1, 2, 3, 9 \end{bmatrix}$			[0, 4, 8, 3, 7, 11, 6, 10, 14, 9, 13, 2, 12, 1, 5]
	[0, 6, 7, 13, 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, 4, 14, 3, 7, 2, 6, 10, 5, 9, 13, 8, 12, 1, 11]
	[0, 6, 12, 13, 9, 5, 11, 2, 3, 14, 10, 1, 7, 8, 4]			
	[0, 1, 3, 2, 4, 5, 6, 8, 7, 9, 10, 11, 13, 12, 14]	) ← New	ontimal	generators
	[0, 1, 3, 2, 9, 5, 6, 8, 7, 14, 10, 11, 13, 12, 4]		optimar	Benerators
	[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]			
[0,1,2,9,4]	[0, 1, 3, 12, 4, 5, 6, 8, 2, 9, 10, 11, 13, 7, 14]			
[0, 1, 3, 2, 4]	[0, 1, 3, 12, 9, 5, 6, 8, 2, 14, 10, 11, 13, 7, 4]			
	$\left[0, 1, 3, 12, 14, 5, 6, 8, 2, 4, 10, 11, 13, 7, 9\right]$			
	[0, 1, 8, 12, 4, 5, 6, 13, 2, 9, 10, 11, 3, 7, 14]			
	$\left[0, 6, 3, 2, 9, 5, 11, 8, 7, 14, 10, 1, 13, 12, 4\right]$			
	[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]			

#### **31 new optimal generators are there!**

Hong-Yeop Song

# 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 recursive construction? If not, how can we get them?