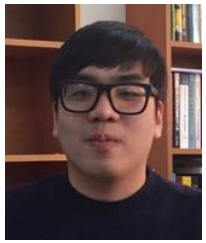
Generalized Milewski sequences
with
perfect autocorrelation/optimal crosscorrelation

(and its relation with **circular Florentine arrays**)

ITA 2019, San Diego, California, USA

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

Yonsei University, Seoul, Korea



based on the recent submission to IEEE IT Trans in Jan 2019

New framework for sequences with perfect autocorrelation and optimal crosscorrelation

Contents of Talk

- Some preliminary concepts
  - Circular Florentine arrays
  - Perfect sequences
  - Interleaved sequences
  - Milewski construction – review
- Proposed generalization
- Concluding remarks

Contents of Talk

- Some preliminary concepts
  - Circular Florentine arrays
  - Perfect sequences
  - Interleaved sequences
  - Milewski construction – review
- Proposed generalization
- Concluding remarks

A RESURRECTION OF
A COMBINATORIAL STRUCTURE
AFTER MORE THAN 30 YEARS

Circular Florentine arrays

A $k \times N$ circular Florentine array is ***equivalent*** to a set of k distinct permutations $\pi_1, \pi_2, \ldots, \pi_k$ of the integers modulo N such that

$$\pi_i(x + \tau) = \pi_j(x)$$

has exactly one solution x

for any two distinct permutations π_i, π_j for any shift τ.

Circular Florentine arrays

A $k \times N$ circular Florentine array is ***equivalent*** to a set of k distinct permutations $\pi_1, \pi_2, \ldots, \pi_k$ of the integers modulo N such that

$$\pi_i(x + \tau) = \pi_j(x)$$

has exactly one solution x

for any two distinct permutations π_i, π_j for any shift τ.

S. W. Golomb and H. Taylor,
Tuscan squares – a new family of combinatorial designs,
Ars Combinatoria, 1985.

more than 30 years ago!

10×11 circular Florentine array

0	1	2	3	4	5	6	7	8	9	a
0	2	4	6	8	a	1	3	5	7	9
0	3	6	9	1	4	7	a	2	5	8
0	4	8	1	5	9	2	6	a	3	7
0	5	a	4	9	3	8	2	7	1	6
0	6	1	7	2	8	3	9	4	a	5
0	7	3	a	6	2	9	5	1	8	4
0	8	5	2	a	7	4	1	9	6	3
0	9	7	5	3	1	a	8	6	4	2
0	a	9	8	7	6	5	4	3	2	1

10×11 circular Tuscan-1 array

0	1	2	3	4	5	6	7	8	9	a
0	2	4	6	8	a	1	3	5	7	9
0	3	6	9	1	4	7	a	2	5	8
0	4	8	1	5	9	2	6	a	3	7
0	5	a	4	9	3	8	2	7	1	6
0	6	1	7	2	8	3	9	4	a	5
0	7	3	a	6	2	9	5	1	8	4
0	8	5	2	a	7	4	1	9	6	3
0	9	7	5	3	1	a	8	6	4	2
0	a	9	8	7	6	5	4	3	2	1

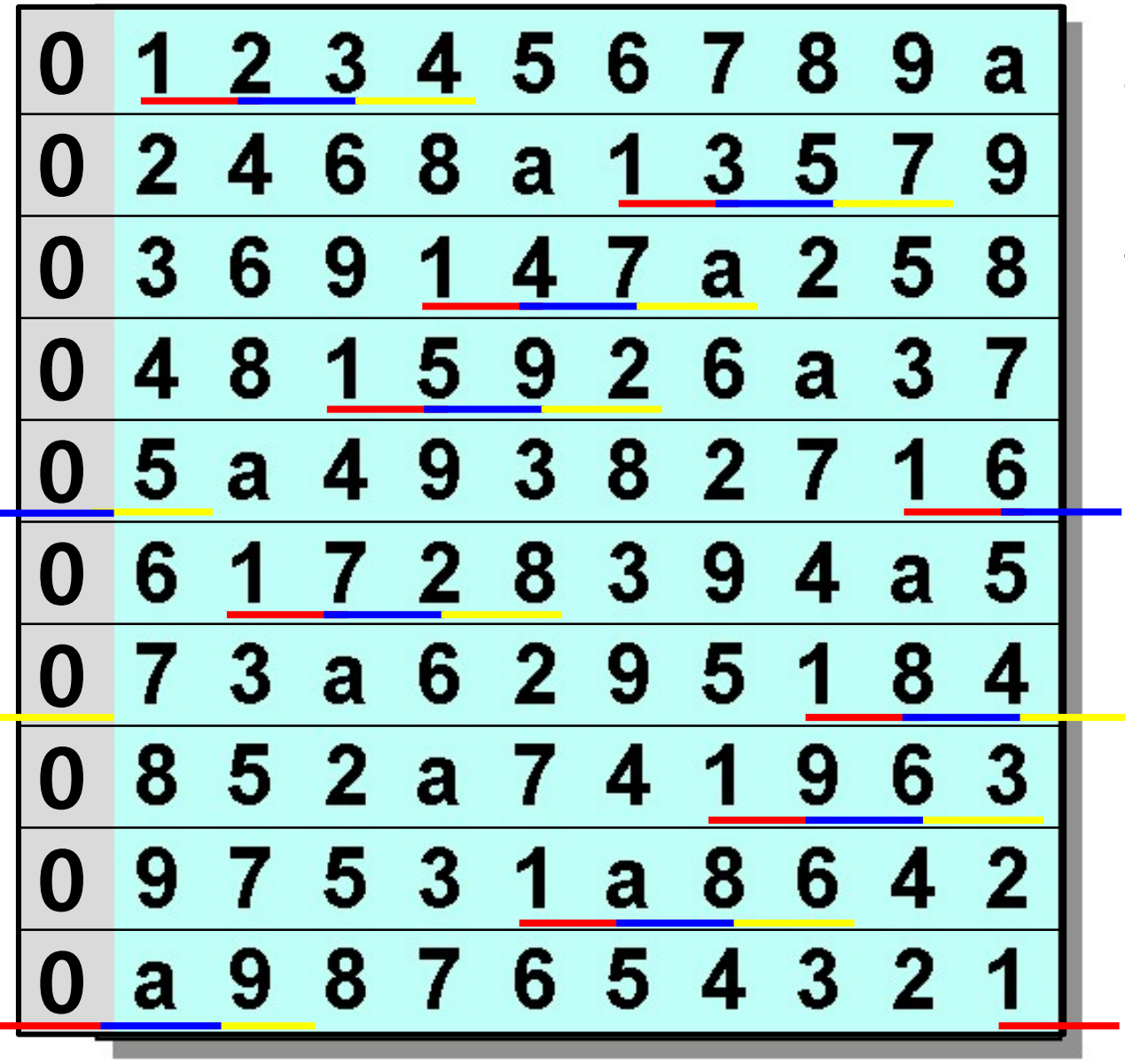
- Each **circular row** is a permutation.
- For any symbol a and distance **1**, the symbols from a in a circular distance **1** are all distinct

10×11 circular Tuscan-2 array

0	1	2	3	4	5	6	7	8	9	a
0	2	4	6	8	a	1	3	5	7	9
0	3	6	9	1	4	7	a	2	5	8
0	4	8	1	5	9	2	6	a	3	7
0	5	a	4	9	3	8	2	7	1	6
0	6	1	7	2	8	3	9	4	a	5
0	7	3	a	6	2	9	5	1	8	4
0	8	5	2	a	7	4	1	9	6	3
0	9	7	5	3	1	a	8	6	4	2
0	a	9	8	7	6	5	4	3	2	1

- Each **circular row** is a permutation.
- In addition, for any symbol $\boldsymbol{a}$ and distance **2**, the symbols from $\boldsymbol{a}$ in a circular distance **2** are all distinct

10×11 circular Tuscan-3 array



- Each **circular row** is a permutation.
- In addition, for any symbol a and distance **3**, the symbols from a in a circular distance **3** are all distinct

10×11 circular Tuscan-4 array

10×11 circular Tuscan-4 array

10×11 circular Tuscan-5 array

10×11 circular Tuscan-4 array

10×11 circular Tuscan-5 array

...

10×11 circular Tuscan-10 array

=10×11 circular Florentine array

10×11 circular Florentine array

0	1	2	3	4	5	6	7	8	9	a
0	2	4	6	8	a	1	3	5	7	9
0	3	6	9	1	4	7	a	2	5	8
0	4	8	1	5	9	2	6	a	3	7
0	5	a	4	9	3	8	2	7	1	6
0	6	1	7	2	8	3	9	4	a	5
0	7	3	a	6	2	9	5	1	8	4
0	8	5	2	a	7	4	1	9	6	3
0	9	7	5	3	1	a	8	6	4	2
0	a	9	8	7	6	5	4	3	2	1

- Each **circular row** is a permutation.
- For **any** symbol α and each distance **d=1,2,…,N-1**, the symbols from α in a **circular distance d** are all distinct

A transform

0	1	2	3	4	5	6	7	8	9	a
0	2	4	6	8	a	1	3	5	7	9
0	3	6	9	1	4	7	a	2	5	8
0	4	8	1	5	9	2	6	a	3	7
0	5	a	4	9	3	8	2	7	1	6
0	6	1	7	2	8	3	9	4	a	5
0	7	3	a	6	2	9	5	1	8	4
0	8	5	2	a	7	4	1	9	6	3
0	9	7	5	3	1	a	8	6	4	2
0	a	9	8	7	6	5	4	3	2	1

We may **rotate** each row without violating the property so that **a common symbol** comes to the left-most column, and **delete** the column.

This gives …

10×10 Florentine square

1	2	3	4	5	6	7	8	9	a
2	4	6	8	a	1	3	5	7	9
3	6	9	1	4	7	a	2	5	8
4	8	1	5	9	2	6	a	3	7
5	a	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	a	5
7	3	a	6	2	9	5	1	8	4
8	5	2	a	7	4	1	9	6	3
9	7	5	3	1	a	8	6	4	2
a	9	8	7	6	5	4	3	2	1

S. W. Golomb and H. Taylor,
Tuscan squares – a new family of combinatorial designs,
Ars Combinatoria, 1985

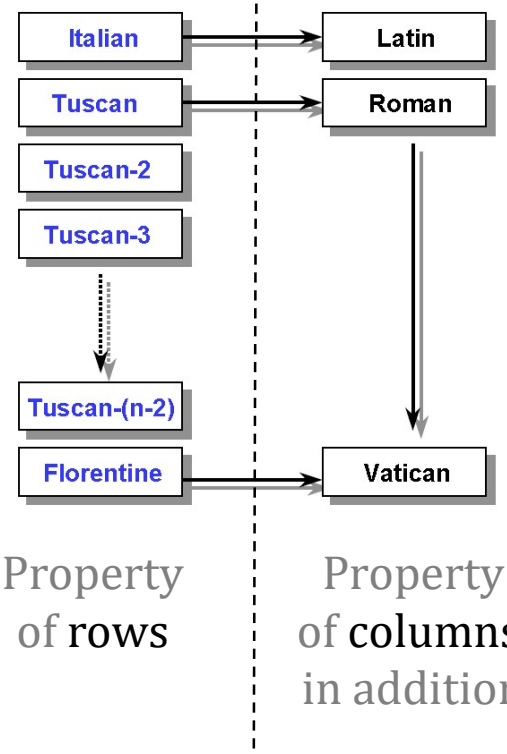
more than 30 years ago!

10×10 Florentine square

1	2	3	4	5	6	7	8	9	a
2	4	6	8	a	1	3	5	7	9
3	6	9	1	4	7	a	2	5	8
4	8	1	5	9	2	6	a	3	7
5	a	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	a	5
7	3	a	6	2	9	5	1	8	4
8	5	2	a	7	4	1	9	6	3
9	7	5	3	1	a	8	6	4	2
a	9	8	7	6	5	4	3	2	1

S. W. Golomb and H. Taylor,
Tuscan squares – a new family of combinatorial designs,
Ars Combinatoria, 1985

more than 30 years ago!

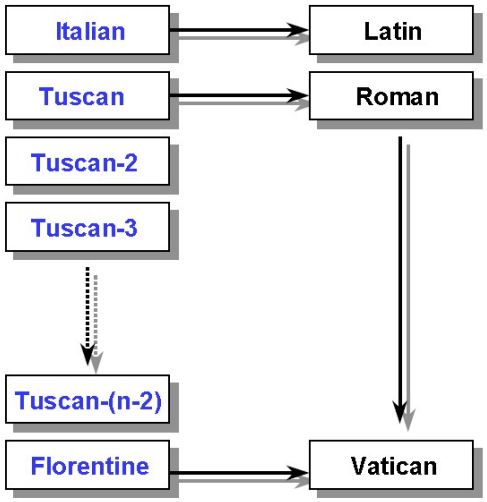


10×10 Florentine square

1	2	3	4	5	6	7	8	9	a
2	4	6	8	a	1	3	5	7	9
3	6	9	1	4	7	a	2	5	8
4	8	1	5	9	2	6	a	3	7
5	a	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	a	5
7	3	a	6	2	9	5	1	8	4
8	5	2	a	7	4	1	9	6	3
9	7	5	3	1	a	8	6	4	2
a	9	8	7	6	5	4	3	2	1

S. W. Golomb and H. Taylor,
Tuscan squares – a new family of combinatorial designs,
Ars Combinatoria, 1985

more than 30 years ago!



H.-Y. Song and **J. H. Dinitz**,
"Tuscan Squares,"
CRC Handbook of Combinatorial Designs, edited by **C. J. Colbourn and J. H. Dinitz,**
CRC Press, pp. 480-484, 1996.

Circular Florentine arrays

- Let $F_c(N)$ be the largest integer such that an $F_c(N) \times N$ circular Florentine array exists. Then,

$$p_{\min} - 1 \leq F_c(N) \leq N - 1$$

.

Circular Florentine arrays

- Let $F_c(N)$ be the largest integer such that an $F_c(N) \times N$ circular Florentine array exists. Then,

$$p_{\min} - 1 \leq F_c(N) \leq N - 1$$

- It is known that
  - if N is prime, then $F_c(N) = N - 1$.

Circular Florentine arrays

- Let $F_c(N)$ be the largest integer such that an $F_c(N) \times N$ circular Florentine array exists. Then,

$$p_{\min} - 1 \leq F_c(N) \leq N - 1$$

- It is known that
  - if N is prime, then $F_c(N) = N - 1$.
  - Especially, if N is even, then $F_c(N) = 1$.

Circular Florentine arrays

- Let $F_c(N)$ be the largest integer such that an $F_c(N) \times N$ circular Florentine array exists. Then,

$$p_{\min} - 1 \leq F_c(N) \leq N - 1$$

- It is known that
  - if N is prime, then $F_c(N) = N - 1$.
  - Especially, if N is even, then $F_c(N) = 1$.
  - For all other odd N, the exact value $F_c(N)$ is widely open.

A 4×15 circular Florentine array

π_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
π_2	0	7	1	8	2	12	3	11	9	4	13	5	14	6	10
π_3	0	4	11	7	10	1	13	9	5	8	3	6	2	14	12
π_4	0	13	7	2	11	6	14	10	3	5	12	9	1	4	8

A 4×15 circular Florentine array

π_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
π_2	0	7	1	8	2	12	3	11	9	4	13	5	14	6	10
π_3	0	4	11	7	10	1	13	9	5	8	3	6	2	14	12
π_4	0	13	7	2	11	6	14	10	3	5	12	9	1	4	8

- $15 = 3 \cdot 5$ and $p_{min} = 3$. Therefore, $2 \leq F_c(15) \leq 14$.
- It turned out that

$$\boldsymbol{F_c(15) = 4}$$

and the above example has 4 rows.

A 4×15 circular Florentine array

π_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
π_2	0	7	1	8	2	12	3	11	9	4	13	5	14	6	10
π_3	0	4	11	7	10	1	13	9	5	8	3	6	2	14	12
π_4	0	13	7	2	11	6	14	10	3	5	12	9	1	4	8

- $15 = 3 \cdot 5$ and $p_{min} = 3$. Therefore, $2 \leq F_c(15) \leq 14$.
- It turned out that

$$\boldsymbol{F_c(15) = 4}$$

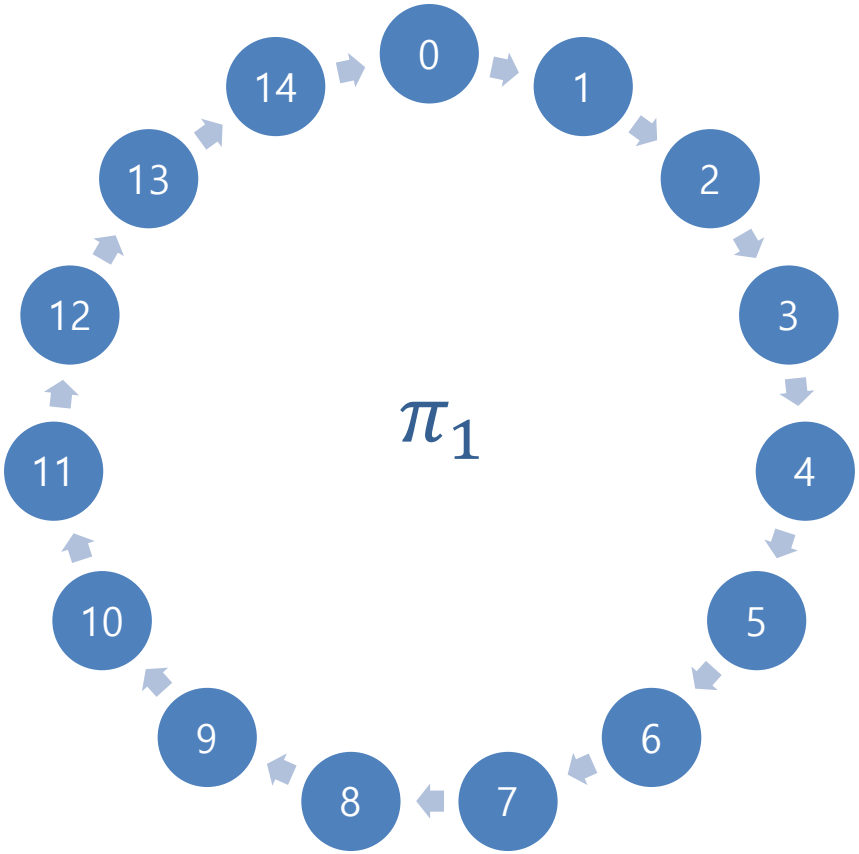
and the above example has 4 rows.

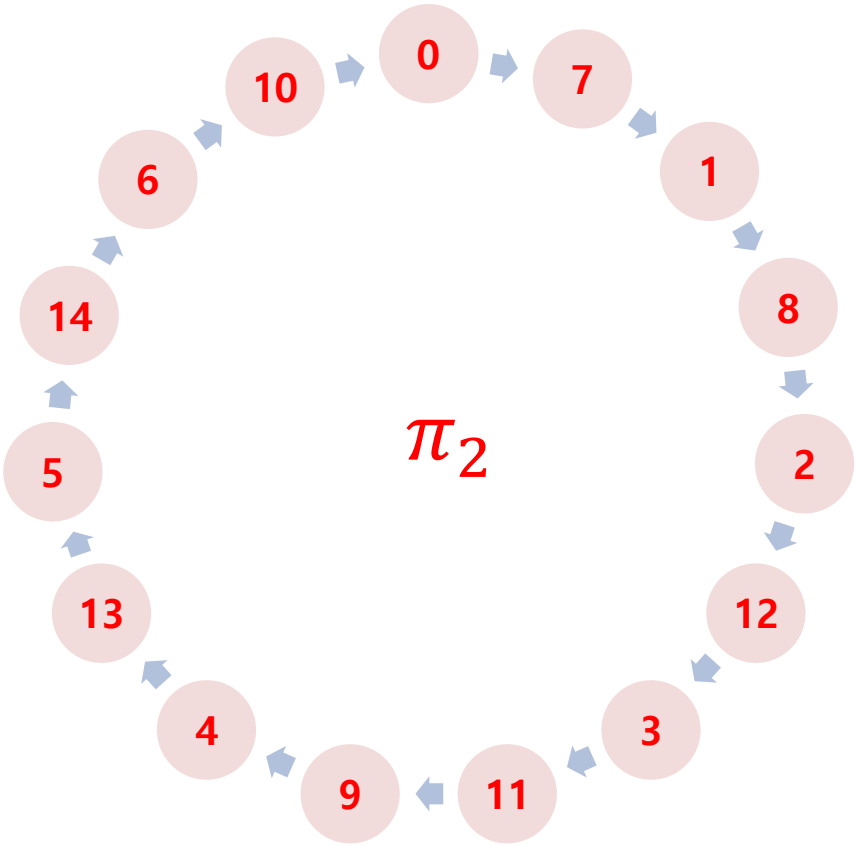
PHD Thesis, USC, by Hong-Yeop Song (1991)
and also, later in
Computers & Mathematics with Applications (2000)

Check

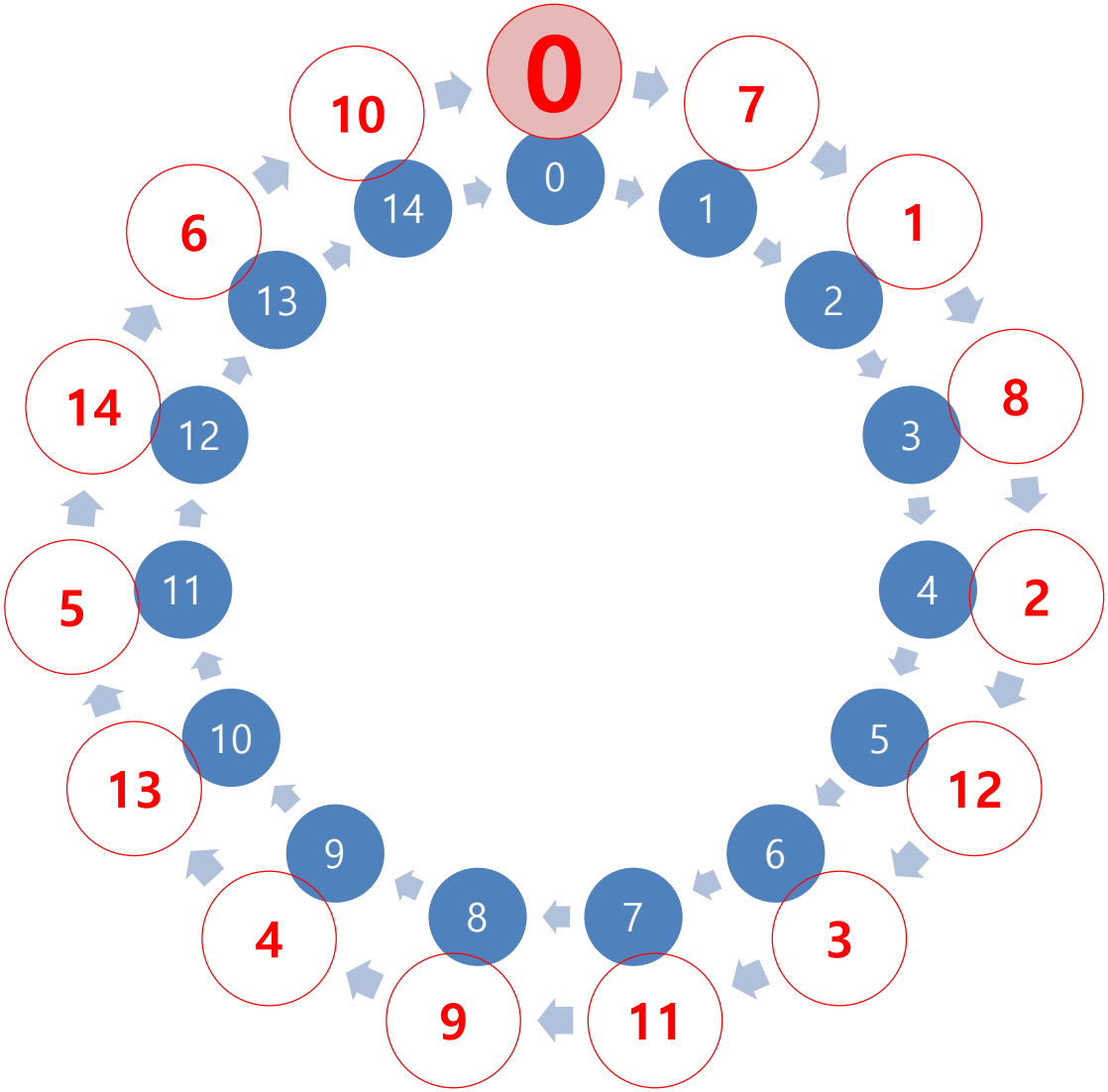
$$\boldsymbol{\pi_2(x+\tau) = \pi_1(x)}$$

has exactly one solution x for any τ

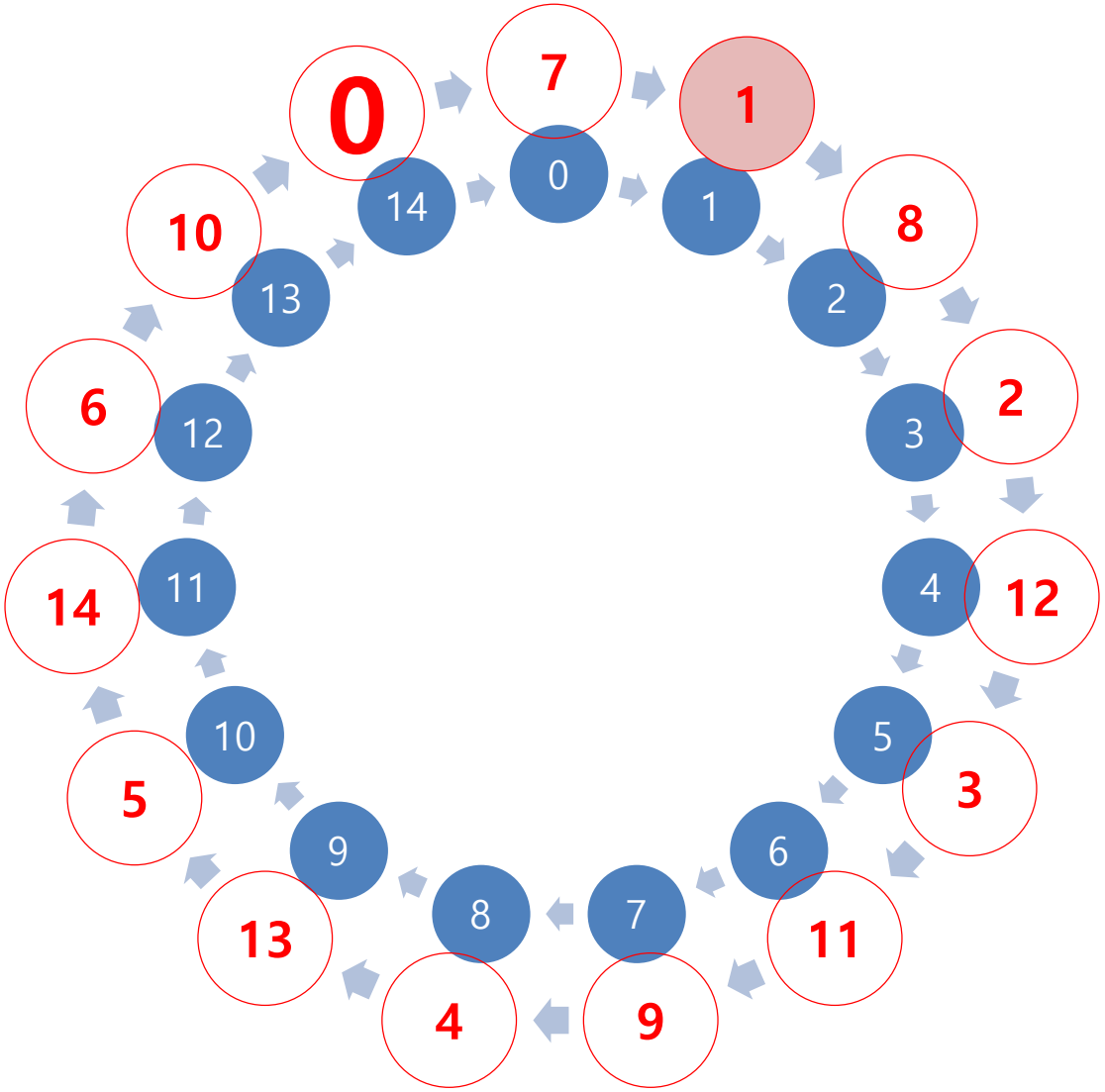




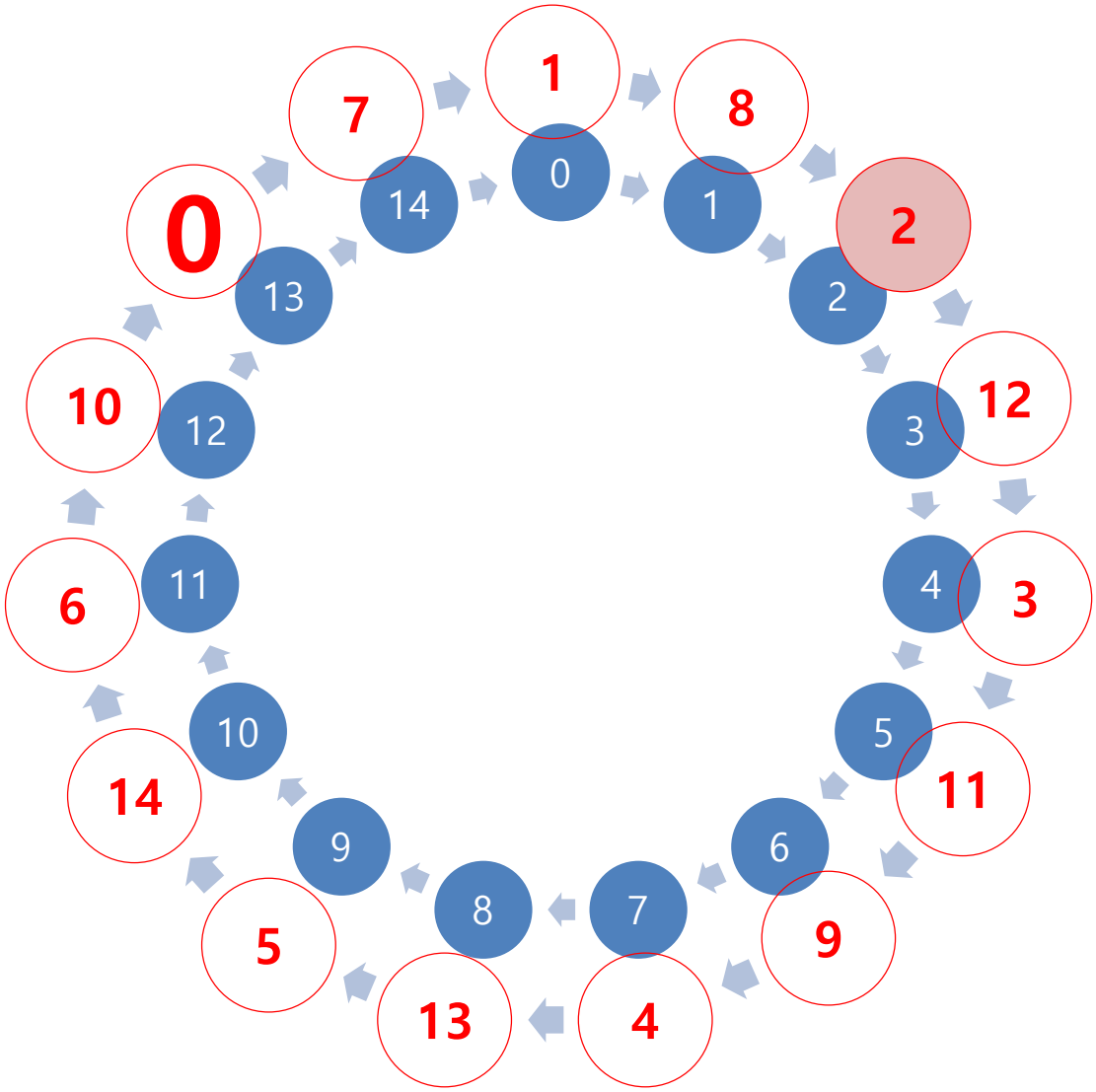
$\tau = 0$



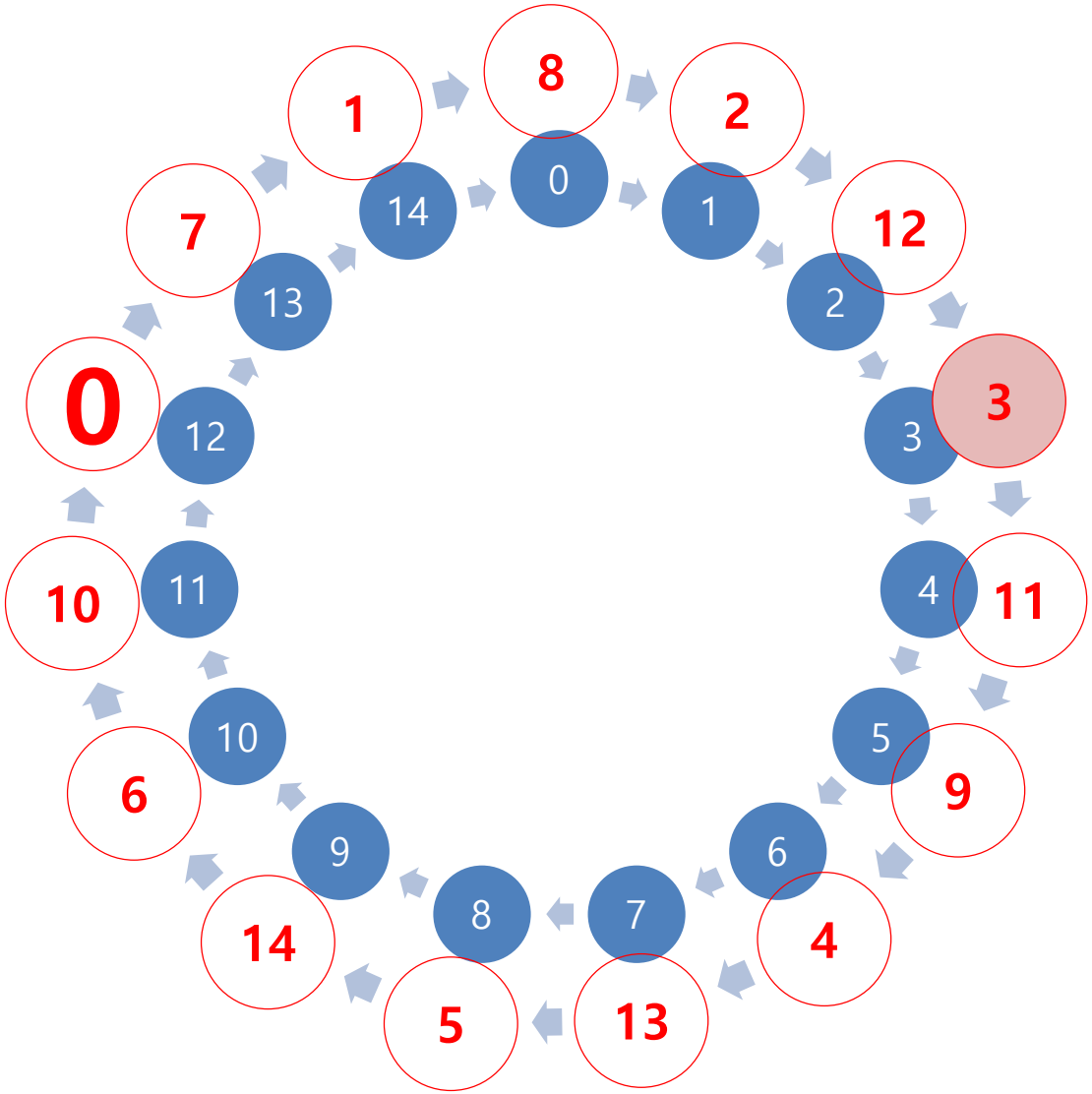
$\tau = 1$



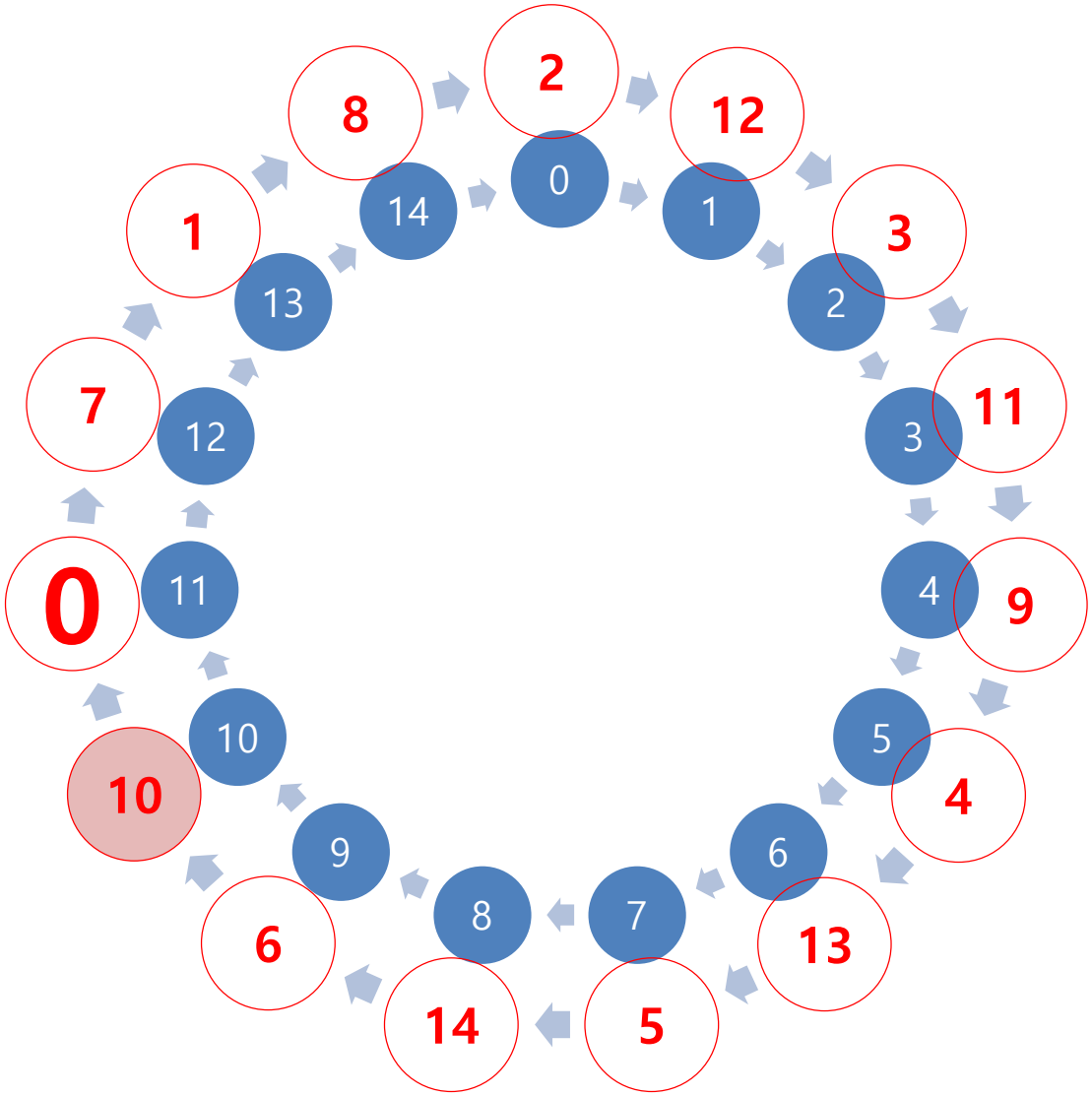
$$\tau = 2$$


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
7
1
8
0
14
1
2
0
13
2
12
10
12
3
12
6
11
4
3
10
5
14
11
9
6
8
7
9
5
13
4

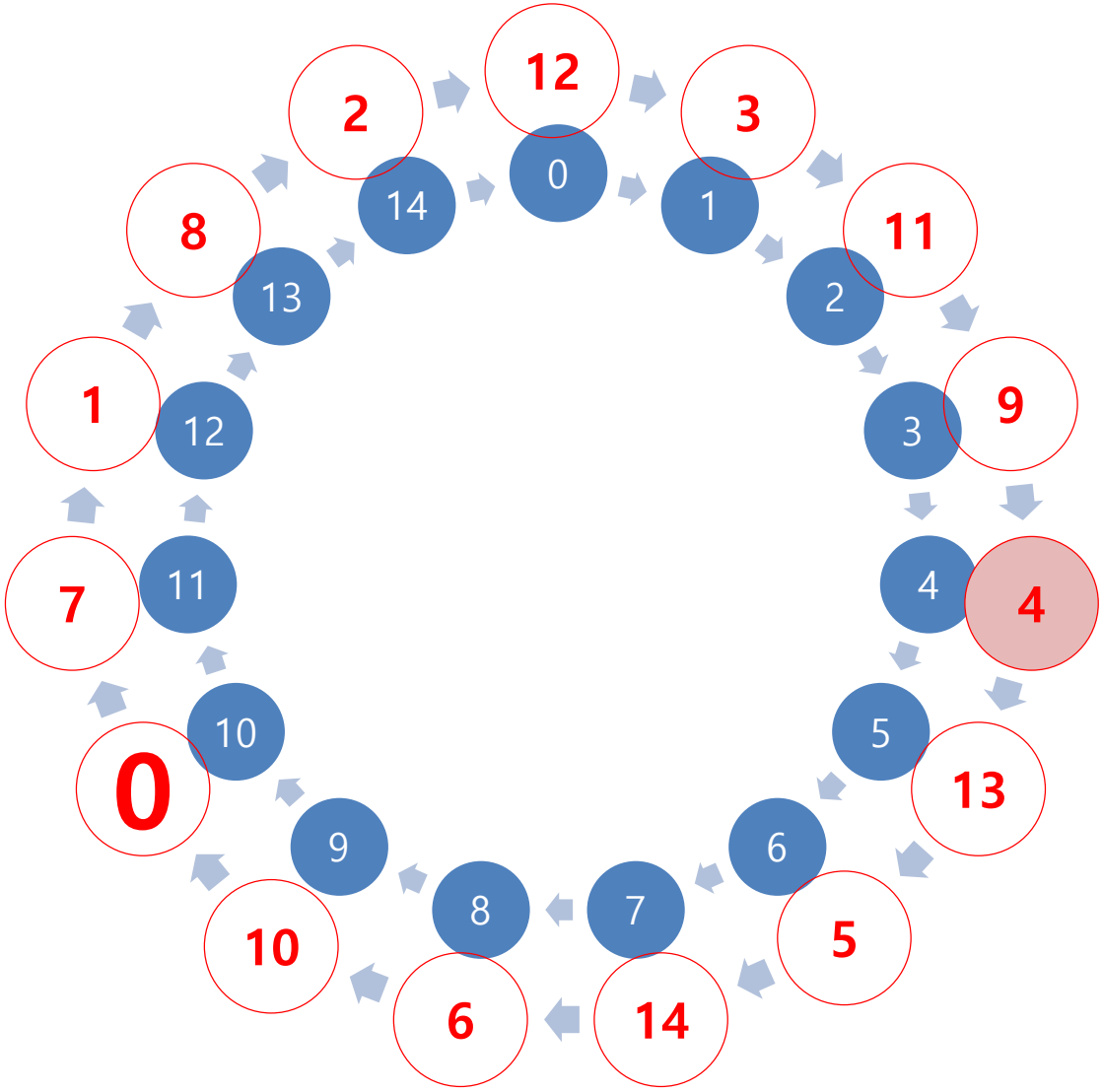
$$\tau = 3$$


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
8
1
2
0
1
12
7
14
2
13
3
0
12
3
4
11
10
11
5
9
10
6
6
9
4
8
7
14
5
13

$$\tau = 4$$

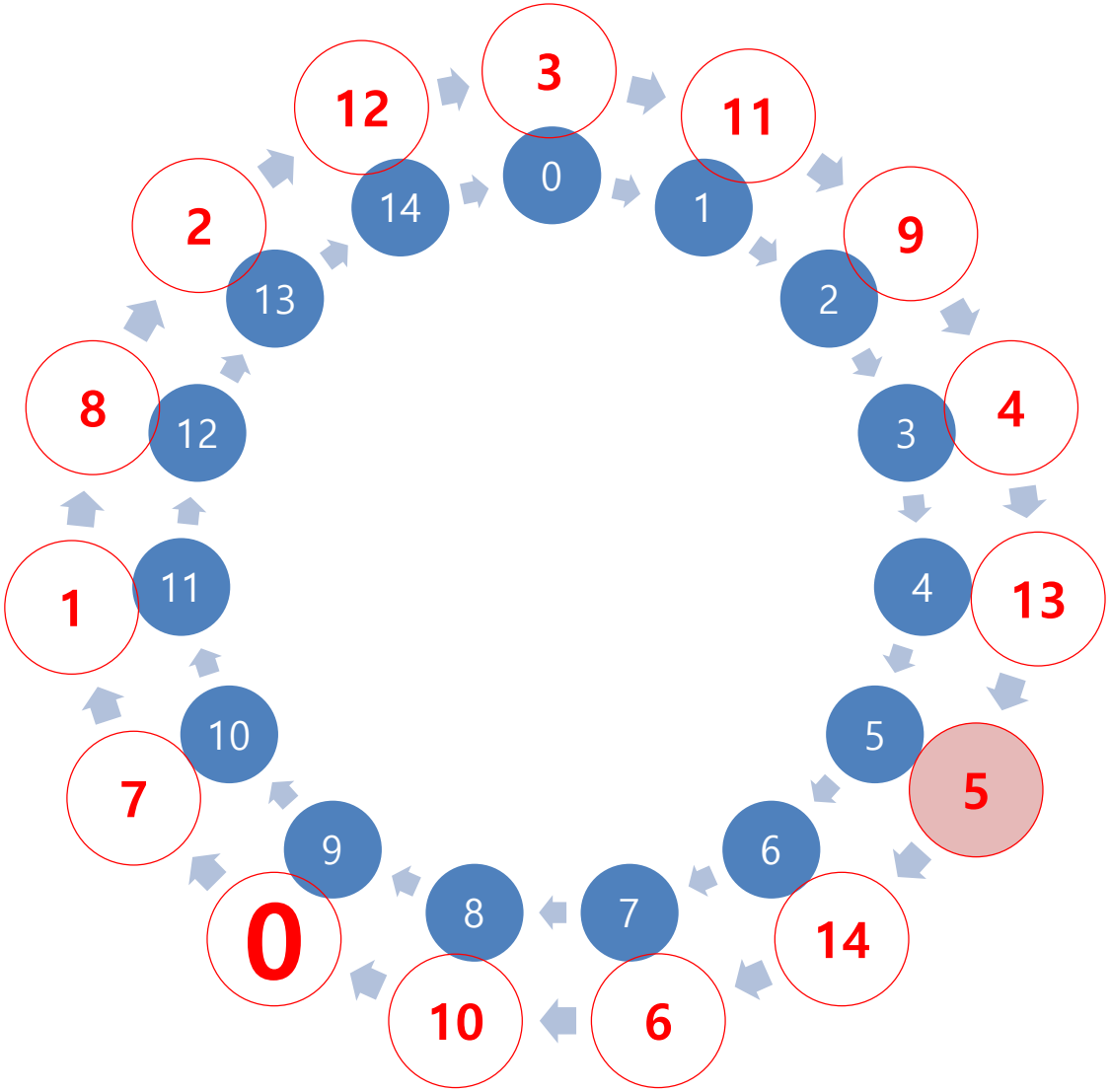


$$\tau = 5$$



$\tau = 6$

etc…



Sequences and Correlation

- For complex-valued sequences $\boldsymbol{x}, \boldsymbol{y}$ of length L, the periodic correlation of $\boldsymbol{x}$ and $\boldsymbol{y}$ at shift $\boldsymbol{\tau}$ is

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

Sequences and Correlation

- For complex-valued sequences $\boldsymbol{x}, \boldsymbol{y}$ of length L, the periodic correlation of $\boldsymbol{x}$ and $\boldsymbol{y}$ at shift $\boldsymbol{\tau}$ is

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

  - If $\boldsymbol{y}$ is a cyclic shift of $\boldsymbol{x}$, it is called **autocorrelation,** and denoted by $\boldsymbol{C_x(\tau)}$
  - Otherwise, it is called **crosscorrelation**

Perfect Sequences

- A sequence $\boldsymbol{x}$ of length $\boldsymbol{L}$ is called **perfect** if

$$C_{\boldsymbol{x}}(\tau) = \begin{cases} \boldsymbol{E}, & \tau \equiv 0 \pmod{L} \\ 0, & \tau \not\equiv 0 \pmod{L} \end{cases}$$

Here, $\boldsymbol{E}$ is called the energy of $\boldsymbol{x}$

Perfect Sequences

- A sequence $\boldsymbol{x}$ of length $\boldsymbol{L}$ is called **perfect** if

$$C_{\boldsymbol{x}}(\tau) = \begin{cases} \boldsymbol{E}, & \tau \equiv 0 \pmod{L} \\ 0, & \tau \not\equiv 0 \pmod{L} \end{cases}$$

Here, $\boldsymbol{E}$ is called the energy of $\boldsymbol{x}$

- (Sarwate, 79) Crosscorrelation of any two perfect sequences of length $\boldsymbol{L}$ with the same energy $\boldsymbol{E}$ is lower bounded by $\boldsymbol{E}/\sqrt{\boldsymbol{L}}$.

Perfect Sequences

- A sequence $\boldsymbol{x}$ of length $\boldsymbol{L}$ is called **perfect** if

$$C_{\boldsymbol{x}}(\tau) = \begin{cases} \boldsymbol{E}, & \tau \equiv 0 \pmod{L} \\ 0, & \tau \not\equiv 0 \pmod{L} \end{cases}$$

Here, $\boldsymbol{E}$ is called the energy of $\boldsymbol{x}$

- (Sarwate, 79) Crosscorrelation of any two perfect sequences of length $\boldsymbol{L}$ with the same energy $\boldsymbol{E}$ is lower bounded by $\boldsymbol{E}/\sqrt{\boldsymbol{L}}$.
  - **An optimal pair** of perfect sequences of length $\boldsymbol{L}$
  - **An optimal set** of perfect sequences of length $\boldsymbol{L}$

Interleaved Sequence

- Consider two sequences $\boldsymbol{s}_0 = \{a, b, c\}$ and $\boldsymbol{s}_1 = \{d, e, f\}$ of length **3** each

Interleaved Sequence

- Consider two sequences $\boldsymbol{s}_0 = \{a, b, c\}$ and $\boldsymbol{s}_1 = \{d, e, f\}$ of length **3** each

- Write each as a column of an array:

$$[\boldsymbol{s}_0, \boldsymbol{s}_1] = \begin{bmatrix} a & d \\ b & e \\ c & f \end{bmatrix}$$

Interleaved Sequence

- Consider two sequences $\boldsymbol{s_0} = \{a, b, c\}$ and $\boldsymbol{s_1} = \{d, e, f\}$ of length **3** each

- Write each as a column of an array:

$$[\boldsymbol{s_0}, \boldsymbol{s_1}] = \begin{bmatrix} a & d \\ b & e \\ c & f \end{bmatrix}$$

- Read the array row-by-row and obtain a sequence of length **6**:

$$\boldsymbol{s} = I(\boldsymbol{s_0}, \boldsymbol{s_1}) = \{a, d, b, e, c, f\}$$

is called **an interleaved sequence** of $\boldsymbol{s_0}$ and $\boldsymbol{s_1}$

History of Perfect Polyphase Sequences

1960's

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

1970's

1980's

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

1990's

P1 code

Alphabet size : N

Period : N^2

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

History of 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

1990's

Popovic
IEEE T-IT, 1992

P1 code
Alphabet size : N
Period : N^2

P2 code
Alphabet size : N
Period : N

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

History of Perfect Polyphase Sequences

1960's

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

1970's

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

Milewski
IBM J. R&D, 1983

1980's

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

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}

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

History of 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

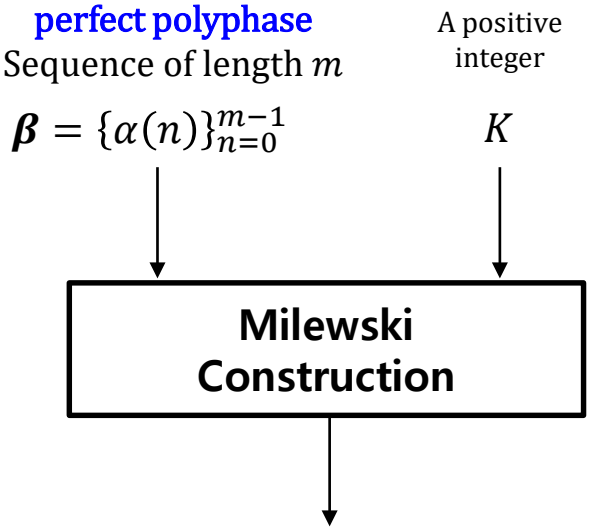
Mow's two unified construction (dissertation 1993, ISSTA 1996)

The original Milewski construction

Length: $m \rightarrow m \cdot m^{2K}$

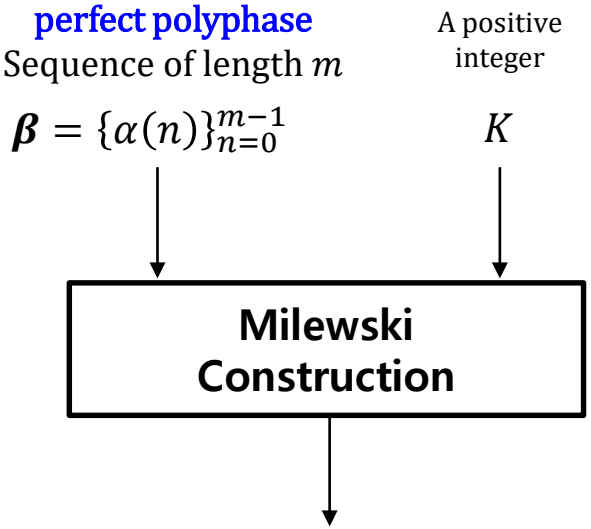
The original Milewski construction

Length: $m \rightarrow m \cdot m^{2K}$



The original Milewski construction

Length: $m \rightarrow m \cdot m^{2K}$



where

$$\boldsymbol{s(n) = \beta(q)\omega^{qr}}$$

$$\omega = e^{-j\frac{2\pi}{m^{1+K}}}$$

Here, we use

$$n = \boldsymbol{qm^{K} + r} \;\leftrightarrow\; \boldsymbol{(q, r)}$$

The original Milewski construction

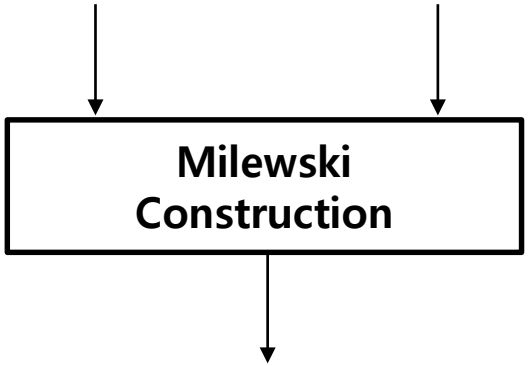
Length: $m \rightarrow m \cdot m^{2K}$

perfect polyphase
Sequence of length m

$$\boldsymbol{\beta} = \{\alpha(n)\}_{n=0}^{m-1}$$

A positive integer

$$K$$



Output perfect polyphase sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{\boldsymbol{m^{2K+1}}-1}$$

where

$$\boldsymbol{s(n) = \beta(q)\omega^{qr}}$$

$$\omega = e^{-j\frac{2\pi}{m^{1+K}}}$$

Here, we use

$$n = \boldsymbol{qm^{K}} + \boldsymbol{r} \;\leftrightarrow\; (\boldsymbol{q}, \boldsymbol{r})$$

$m \cdot m^K \times m^K$ array form of $\boldsymbol{s}$

The original Milewski construction

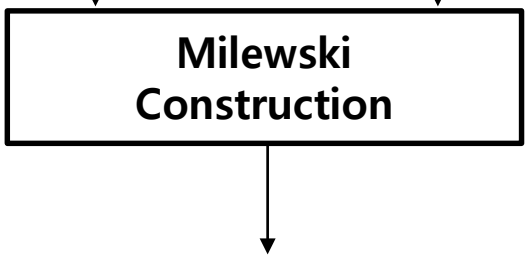
Length: $m \rightarrow m \cdot m^{2K}$

perfect polyphase
Sequence of length m

$$\boldsymbol{\beta} = \{\alpha(n)\}_{n=0}^{m-1}$$

A positive integer

$$K$$



Output perfect polyphase sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{\boldsymbol{m^{2K+1}}-1}$$

where

$$\boldsymbol{s(n) = \beta(q)\omega^{qr}}$$

$$\omega = e^{-j\frac{2\pi}{m^{1+K}}}$$

Here, we use

$$n = \boldsymbol{qm^K} + \boldsymbol{r} \;\leftrightarrow\; (\boldsymbol{q}, \boldsymbol{r})$$

$m \cdot m^K \times m^K$ array form of $\boldsymbol{s}$

$$\begin{bmatrix}
\beta(0) & \beta(0) & \cdots & \beta(0) \\
\beta(1) & \beta(1) & \cdots & \beta(1) \\
\beta(2) & \beta(2) & \cdots & \beta(2) \\
\vdots & \vdots & & \vdots \\
\beta(m-1) & \beta(m-1) & \cdots & \beta(m-1) \\
\vdots & \vdots & & \vdots \\
\beta(0) & \beta(0) & \cdots & \beta(0) \\
\beta(1) & \beta(1) & \cdots & \beta(1) \\
\beta(2) & \beta(2) & \cdots & \beta(2) \\
\vdots & \vdots & & \vdots \\
\beta(m-1) & \beta(m-1) & \cdots & \beta(m-1)
\end{bmatrix}$$

Input sequence $\boldsymbol{\beta}$ of period m is repeated m^K times

The original Milewski construction

Length: $m \rightarrow m \cdot m^{2K}$

perfect polyphase
Sequence of length m

$$\boldsymbol{\beta} = \{\alpha(n)\}_{n=0}^{m-1}$$

A positive integer

$$K$$

Milewski Construction

Output perfect polyphase sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{m^{2K+1}-1}$$

where

$$\boldsymbol{s(n) = \beta(q)\omega^{qr}}$$

$$\boldsymbol{\omega = e^{-j\frac{2\pi}{m^{1+K}}}}$$

Here, we use

$$n = \boldsymbol{qm^K + r} \leftrightarrow (\boldsymbol{q}, \boldsymbol{r})$$

$m \cdot m^K \times m^K$ array form of $\boldsymbol{s}$

$$\begin{bmatrix}
\beta(0) \times 1 & \beta(0) \times 1 & \cdots & \beta(0) \times 1 \\
\beta(1) \times 1 & \beta(1) \times \omega & \cdots & \beta(1) \times (\omega^{N-1})^{1} \\
\beta(2) \times 1 & \beta(2) \times \omega^{2} & \cdots & \beta(2) \times (\omega^{N-1})^{2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(m-1) \times 1 & \beta(m-1) \times \omega^{m-1} & \cdots & \beta(m-1) \times (\omega^{N-1})^{m-1} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(0) \times 1 & \beta(0) \times \omega^{m(N-1)} & \cdots & \beta(0) \times (\omega^{N-1})^{m(N-1)} \\
\beta(1) \times 1 & \beta(1) \times \omega^{m(N-1)+1} & \cdots & \beta(1) \times (\omega^{N-1})^{m(N-1)+1} \\
\beta(2) \times 1 & \beta(2) \times \omega^{m(N-1)+2} & \cdots & \beta(2) \times (\omega^{N-1})^{m(N-1)+2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(m-1) \times 1 & \beta(m-1) \times \omega^{mN-1} & \cdots & \beta(m-1) \times (\omega^{N-1})^{mN-1}
\end{bmatrix}$$

Input sequence $\boldsymbol{\beta}$ of period m is repeated m^K times

The original Milewski construction

Length: $m \rightarrow m \cdot m^{2K}$

perfect polyphase
Sequence of length m

$$\boldsymbol{\beta} = \{\alpha(n)\}_{n=0}^{m-1}$$

A positive integer

$$K$$

Milewski Construction

Output perfect polyphase sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{m^{2K+1}-1}$$

where

$$\boldsymbol{s(n) = \beta(q)\omega^{qr}}$$

$$\boldsymbol{\omega = e^{-j\frac{2\pi}{m^{1+K}}}}$$

Here, we use

$$n = \boldsymbol{qm^K + r} \leftrightarrow (\boldsymbol{q}, \boldsymbol{r})$$

$m \cdot m^K \times m^K$ array form of $\boldsymbol{s}$

$$\begin{bmatrix}
\beta(0) \times 1 & \beta(0) \times 1 & \cdots & \beta(0) \times 1 \\
\beta(1) \times 1 & \beta(1) \times \omega & \cdots & \beta(1) \times (\omega^{N-1})^{1} \\
\beta(2) \times 1 & \beta(2) \times \omega^{2} & \cdots & \beta(2) \times (\omega^{N-1})^{2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(m-1) \times 1 & \beta(m-1) \times \omega^{m-1} & \cdots & \beta(m-1) \times (\omega^{N-1})^{m-1} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(0) \times 1 & \beta(0) \times \omega^{m(N-1)} & \cdots & \beta(0) \times (\omega^{N-1})^{m(N-1)} \\
\beta(1) \times 1 & \beta(1) \times \omega^{m(N-1)+1} & \cdots & \beta(1) \times (\omega^{N-1})^{m(N-1)+1} \\
\beta(2) \times 1 & \beta(2) \times \omega^{m(N-1)+2} & \cdots & \beta(2) \times (\omega^{N-1})^{m(N-1)+2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(m-1) \times 1 & \beta(m-1) \times \omega^{mN-1} & \cdots & \beta(m-1) \times (\omega^{N-1})^{mN-1}
\end{bmatrix}$$

Input sequence $\boldsymbol{\beta}$ of period m is repeated m^K times

Here, $N = m^K$ and the exponent runs from 0 to $mN - 1$

The original Milewski construction

Length: $m \rightarrow m \cdot m^{2K}$

perfect polyphase Sequence of length m

$$\boldsymbol{\beta} = \{\alpha(n)\}_{n=0}^{m-1}$$

A positive integer

$$K$$

Milewski Construction

Output **perfect polyphase** sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{m^{2K+1}-1}$$

where

$$\boldsymbol{s(n) = \beta(q)\omega^{qr}}$$

$$\boldsymbol{\omega = e^{-j\frac{2\pi}{m^{1+K}}}}$$

Here, we use

$$n = \boldsymbol{qm^K + r} \leftrightarrow (\boldsymbol{q}, \boldsymbol{r})$$

the exponent runs from 0 to $N-1$

$m \cdot m^K \times m^K$ array form of $\boldsymbol{s}$

$$\begin{bmatrix}
\beta(0) \times 1 & \beta(0) \times 1 & \cdots & \beta(0) \times 1 \\
\beta(1) \times 1 & \beta(1) \times \omega & \cdots & \beta(1) \times (\omega^{N-1})^{1} \\
\beta(2) \times 1 & \beta(2) \times \omega^{2} & \cdots & \beta(2) \times (\omega^{N-1})^{2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(m-1) \times 1 & \beta(m-1) \times \omega^{m-1} & \cdots & \beta(m-1) \times (\omega^{N-1})^{m-1} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(0) \times 1 & \beta(0) \times \omega^{m(N-1)} & \cdots & \beta(0) \times (\omega^{N-1})^{m(N-1)} \\
\beta(1) \times 1 & \beta(1) \times \omega^{m(N-1)+1} & \cdots & \beta(1) \times (\omega^{N-1})^{m(N-1)+1} \\
\beta(2) \times 1 & \beta(2) \times \omega^{m(N-1)+2} & \cdots & \beta(2) \times (\omega^{N-1})^{m(N-1)+2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta(m-1) \times 1 & \beta(m-1) \times \omega^{mN-1} & \cdots & \beta(m-1) \times (\omega^{N-1})^{mN-1}
\end{bmatrix}$$

Input sequence $\boldsymbol{\beta}$ of period m is repeated m^K times

Contents of Talk

- Some preliminary concepts
  - Circular Florentine arrays
  - Perfect sequences
  - Interleaved sequences
  - Milewski construction – review

A RESURRECTION OF
A COMBINATORIAL STRUCTURE
AFTER MORE THAN 30 YEARS

- **Proposed generalization**

- Concluding remarks

Our framework

(A special type of interleaved sequences)

not necessarily **polyphase**
not necessarily **all distinct**

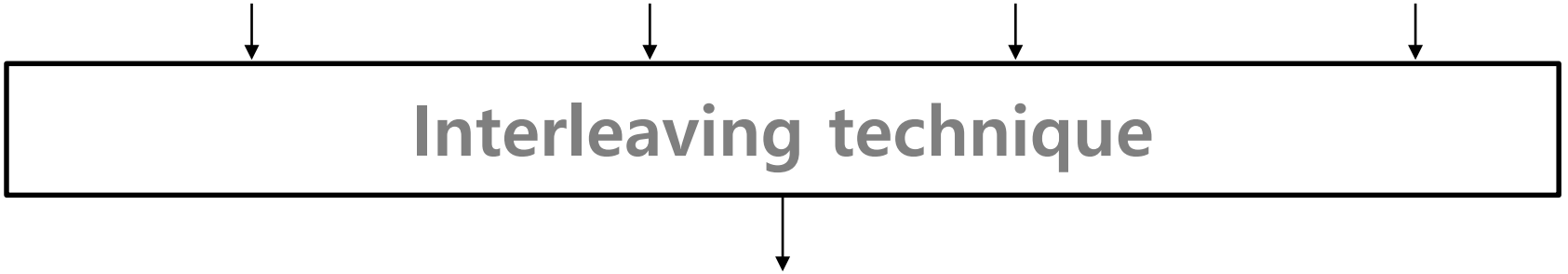
A collection of N sequence of length m	A positive integer	A **polyphase** sequence of length N	A function
$\boldsymbol{B} = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_N\}$	N	$\boldsymbol{\mu}$	$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{\boldsymbol{mN}}$
			π

Our framework

(A special type of interleaved sequences)

not necessarily **polyphase**
not necessarily **all distinct**

A collection of N sequence of length m	A positive integer	A **polyphase** sequence of length N	A function
$\boldsymbol{B} = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \dots, \boldsymbol{\beta}_N\}$	N	$\boldsymbol{\mu}$	$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{mN}$ π



Output sequence $S = \{\boldsymbol{s(n)}\}_{n=0}^{mN^2-1}$

where $\boldsymbol{s(n)} = \boldsymbol{\mu(r)\beta_r(q)\omega^{q\pi(r)}}$

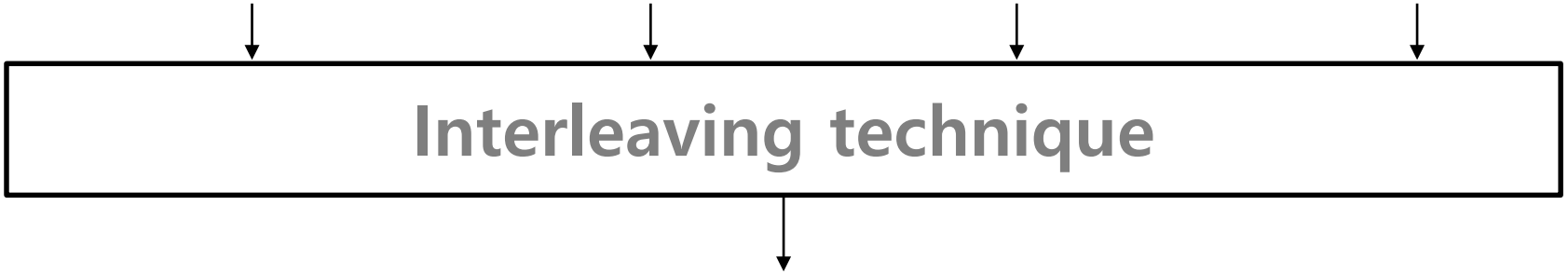
with $\boldsymbol{n = qN + r}$, and $\boldsymbol{\omega = \exp(-j2\pi/mN)}$.

Our framework

(A special type of interleaved sequences)

not necessarily **polyphase**
not necessarily **all distinct**

A collection of N sequence of length m	A positive integer	A **polyphase** sequence of length N	A function
$\boldsymbol{B} = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \dots, \boldsymbol{\beta}_N\}$	N	$\boldsymbol{\mu}$	$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{mN}$ π



Output sequence $S = \{\boldsymbol{s(n)}\}_{n=0}^{mN^2-1}$

where $\boldsymbol{s(n)} = \boldsymbol{\mu(r)\beta_r(q)\omega^{q\pi(r)}}$

with $\boldsymbol{n = qN + r}$, and $\boldsymbol{\omega = \exp(-j2\pi/mN)}$.

Definition. We define $\boldsymbol{\mathcal{A}(B, \pi)}$ be a family of interleaved sequences constructed by the above procedure using all possible polyphase sequences $\boldsymbol{\mu}$.

Array Form

Assume that $\boldsymbol{\mu}$ is the all-one sequence,

※ $\omega = e^{-j\frac{2\pi}{mN}}$

Array Form

Assume that $\boldsymbol{\mu}$ is the all-one sequence,

※ $\omega = e^{-j\frac{2\pi}{mN}}$

Column index $\boldsymbol{r = 0, 1, 2, \ldots, N-1}$

Row index $\boldsymbol{q = 0, 1, 2, \ldots, mN-1}$

Array Form

Assume that $\boldsymbol{\mu}$ is the all-one sequence,

※ $\omega = e^{-j\frac{2\pi}{mN}}$

Column index $\boldsymbol{r = 0, 1, 2, \ldots, N-1}$

Row index $\boldsymbol{q = 0, 1, 2, \ldots, mN-1}$

$\beta_0(0)$	$\beta_1(0)$	$\cdots$	$\beta_{N-1}(0)$
$\beta_0(1)$	$\beta_1(1)$	$\cdots$	$\beta_{N-1}(1)$
$\beta_0(2)$	$\beta_1(2)$	$\cdots$	$\beta_{N-1}(2)$
$\vdots$	$\vdots$		$\vdots$
$\beta_0(m-1)$	$\beta_1(m-1)$	$\cdots$	$\beta_{N-1}(m-1)$
$\vdots$	$\vdots$		$\vdots$
$\beta_0(0)$	$\beta_1(0)$	$\cdots$	$\beta_{N-1}(0)$
$\beta_0(1)$	$\beta_1(1)$	$\cdots$	$\beta_{N-1}(1)$
$\beta_0(2)$	$\beta_1(2)$	$\cdots$	$\beta_{N-1}(2)$
$\vdots$	$\vdots$		$\vdots$
$\beta_0(m-1)$	$\beta_1(m-1)$	$\cdots$	$\beta_{N-1}(m-1)$

Input sequence $\boldsymbol{\beta}_0$ of period m Repeating N times

Input sequence $\boldsymbol{\beta}_1$ of period m Repeating N times

Input sequence $\boldsymbol{\beta}_{N-1}$ of period m Repeating N times

Array Form

Assume that $\boldsymbol{\mu}$ is the all-one sequence,

※ $\omega = e^{-j\frac{2\pi}{mN}}$

Column index $\boldsymbol{r = 0, 1, 2, \dots, N-1}$

Row index $\boldsymbol{q = 0, 1, 2, \dots, mN-1}$

$$
\begin{array}{llll}
\beta_0(0) \times (\omega^{\pi(0)})^{0} & \beta_1(0) \times (\omega^{\pi(1)})^{0} & \cdots & \beta_{N-1}(0) \times (\omega^{\pi(N-1)})^{0} \\
\beta_0(1) \times (\omega^{\pi(0)})^{1} & \beta_1(1) \times (\omega^{\pi(1)})^{1} & \cdots & \beta_{N-1}(1) \times (\omega^{\pi(N-1)})^{1} \\
\beta_0(2) \times (\omega^{\pi(0)})^{2} & \beta_1(2) \times (\omega^{\pi(1)})^{2} & \cdots & \beta_{N-1}(2) \times (\omega^{\pi(N-1)})^{2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta_0(m-1) \times (\omega^{\pi(0)})^{m-1} & \beta_1(m-1) \times (\omega^{\pi(1)})^{m-1} & \cdots & \beta_{N-1}(m-1) \times (\omega^{\pi(N-1)})^{m-1} \\
\vdots & \vdots & \ddots & \vdots \\
\beta_0(0) \times (\omega^{\pi(0)})^{m(N-1)} & \beta_1(0) \times (\omega^{\pi(1)})^{m(N-1)} & \cdots & \beta_{N-1}(0) \times (\omega^{\pi(N-1)})^{m(N-1)} \\
\beta_0(1) \times (\omega^{\pi(0)})^{m(N-1)+1} & \beta_1(1) \times (\omega^{\pi(1)})^{m(N-1)+1} & \cdots & \beta_{N-1}(1) \times (\omega^{\pi(N-1)})^{m(N-1)+1} \\
\beta_0(2) \times (\omega^{\pi(0)})^{m(N-1)+2} & \beta_1(2) \times (\omega^{\pi(1)})^{m(N-1)+2} & \cdots & \beta_{N-1}(2) \times (\omega^{\pi(N-1)})^{m(N-1)+2} \\
\vdots & \vdots & \ddots & \vdots \\
\beta_0(m-1) \times (\omega^{\pi(0)})^{mN-1} & \beta_1(m-1) \times (\omega^{\pi(1)})^{mN-1} & \cdots & \beta_{N-1}(m-1) \times (\omega^{\pi(N-1)})^{mN-1}
\end{array}
$$

Input function $\pi: \mathbb{Z}_N \longrightarrow \mathbb{Z}_{mN}$

Array Form

Assume that $\boldsymbol{\mu}$ is the all-one sequence,

the exponent runs from $\pi(0)$ to $\pi(N-1)$

Column index $\boldsymbol{r = 0, 1, 2, \dots, N-1}$

Row index $\boldsymbol{q = 0, 1, 2, \dots, mN-1}$

$$
\begin{array}{cccccc}
\beta_0(0) & \times (\omega^{\pi(0)})^{0} & \beta_1(0) & \times (\omega^{\pi(1)})^{0} & \cdots & \beta_{N-1}(0) \times (\omega^{\pi(N-1)})^{0} \\
\beta_0(1) & \times (\omega^{\pi(0)})^{1} & \beta_1(1) & \times (\omega^{\pi(1)})^{1} & \cdots & \beta_{N-1}(1) \times (\omega^{\pi(N-1)})^{1} \\
\beta_0(2) & \times (\omega^{\pi(0)})^{2} & \beta_1(2) & \times (\omega^{\pi(1)})^{2} & \cdots & \beta_{N-1}(2) \times (\omega^{\pi(N-1)})^{2} \\
\vdots & & \vdots & & \ddots & \vdots \\
\beta_0(m-1) & \times (\omega^{\pi(0)})^{(m-1)} & \beta_1(m-1) & \times (\omega^{\pi(1)})^{m-1} & \cdots & \beta_{N-1}(m-1) \times (\omega^{\pi(N-1)})^{m-1} \\
\vdots & & \vdots & & \ddots & \vdots \\
\beta_0(0) & \times (\omega^{\pi(0)})^{m(N-1)} & \beta_1(0) & \times (\omega^{\pi(1)})^{m(N-1)} & \cdots & \beta_{N-1}(0) \times (\omega^{\pi(N-1)})^{m(N-1)} \\
\beta_0(1) & \times (\omega^{\pi(0)})^{m(N-1)+1} & \beta_1(1) & \times (\omega^{\pi(1)})^{m(N-1)+1} & \cdots & \beta_{N-1}(1) \times (\omega^{\pi(N-1)})^{m(N-1)+1} \\
\beta_0(2) & \times (\omega^{\pi(0)})^{m(N-1)+2} & \beta_1(2) & \times (\omega^{\pi(1)})^{m(N-1)+2} & \cdots & \beta_{N-1}(2) \times (\omega^{\pi(N-1)})^{m(N-1)+2} \\
\vdots & & \vdots & & \ddots & \vdots \\
\beta_0(m-1) & \times (\omega^{\pi(0)})^{mN-1} & \beta_1(m-1) & \times (\omega^{\pi(1)})^{mN-1} & \cdots & \beta_{N-1}(m-1) \times (\omega^{\pi(N-1)})^{mN-1}
\end{array}
$$

Array Form

Assume that $\boldsymbol{\mu}$ is the all-one sequence,

※ $\omega = e^{-j\frac{2\pi}{mN}}$

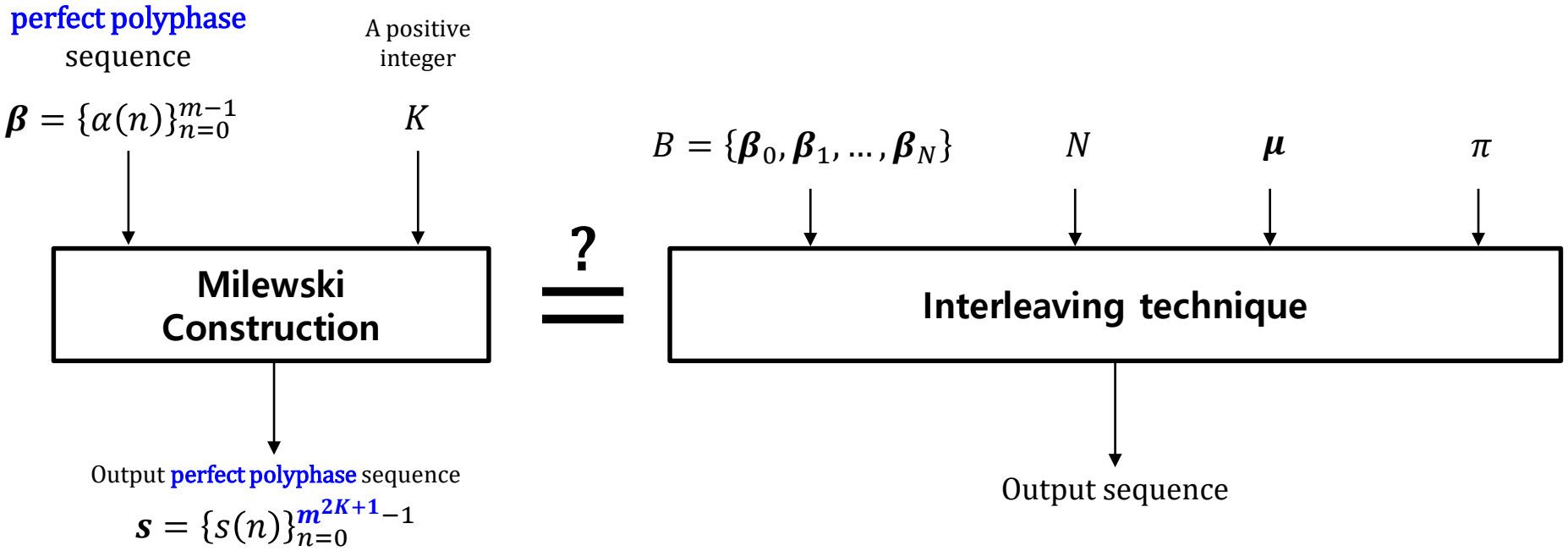
Column index $\boldsymbol{r = 0, 1, 2, \ldots, N-1}$

Row index $\boldsymbol{q = 0, 1, 2, \ldots, mN-1}$

$$
\begin{array}{llll}
\beta_0(0) & \times \left(\omega^{\pi(0)}\right)^{0} & \beta_1(0) & \times \left(\omega^{\pi(1)}\right)^{0} \quad \cdots \quad \beta_{N-1}(0) \times \left(\omega^{\pi(N-1)}\right)^{0} \\
\beta_0(1) & \times \left(\omega^{\pi(0)}\right)^{1} & \beta_1(1) & \times \left(\omega^{\pi(1)}\right)^{1} \quad \cdots \quad \beta_{N-1}(1) \times \left(\omega^{\pi(N-1)}\right)^{1} \\
\beta_0(2) & \times \left(\omega^{\pi(0)}\right)^{2} & \beta_1(2) & \times \left(\omega^{\pi(1)}\right)^{2} \quad \cdots \quad \beta_{N-1}(2) \times \left(\omega^{\pi(N-1)}\right)^{2} \\
 & \vdots & & \vdots \quad \ddots \quad \vdots \\
\beta_0(m-1) & \times \left(\omega^{\pi(0)}\right)^{(m-1)} & \beta_1(m-1) & \times \left(\omega^{\pi(1)}\right)^{m-1} \quad \cdots \quad \beta_{N-1}(m-1) \times \left(\omega^{\pi(N-1)}\right)^{m-1} \\
 & \vdots & & \vdots \quad \ddots \quad \vdots \\
\beta_0(0) & \times \left(\omega^{\pi(0)}\right)^{m(N-1)} & \beta_1(0) & \times \left(\omega^{\pi(1)}\right)^{m(N-1)} \quad \cdots \quad \beta_{N-1}(0) \times \left(\omega^{\pi(N-1)}\right)^{m(N-1)} \\
\beta_0(1) & \times \left(\omega^{\pi(0)}\right)^{m(N-1)+1} & \beta_1(1) & \times \left(\omega^{\pi(1)}\right)^{m(N-1)+1} \quad \cdots \quad \beta_{N-1}(1) \times \left(\omega^{\pi(N-1)}\right)^{m(N-1)+1} \\
\beta_0(2) & \times \left(\omega^{\pi(0)}\right)^{m(N-1)+2} & \beta_1(2) & \times \left(\omega^{\pi(1)}\right)^{m(N-1)+2} \quad \cdots \quad \beta_{N-1}(2) \times \left(\omega^{\pi(N-1)}\right)^{m(N-1)+2} \\
 & \vdots & & \vdots \quad \ddots \quad \vdots \\
\beta_0(m-1) & \times \left(\omega^{\pi(0)}\right)^{mN-1} & \beta_1(m-1) & \times \left(\omega^{\pi(1)}\right)^{mN-1} \quad \cdots \quad \beta_{N-1}(m-1) \times \left(\omega^{\pi(N-1)}\right)^{mN-1}
\end{array}
$$

Here, the exponent of $\boldsymbol{\omega^{\pi(r)}}$ runs from $\boldsymbol{0}$ to $\boldsymbol{mN-1}$

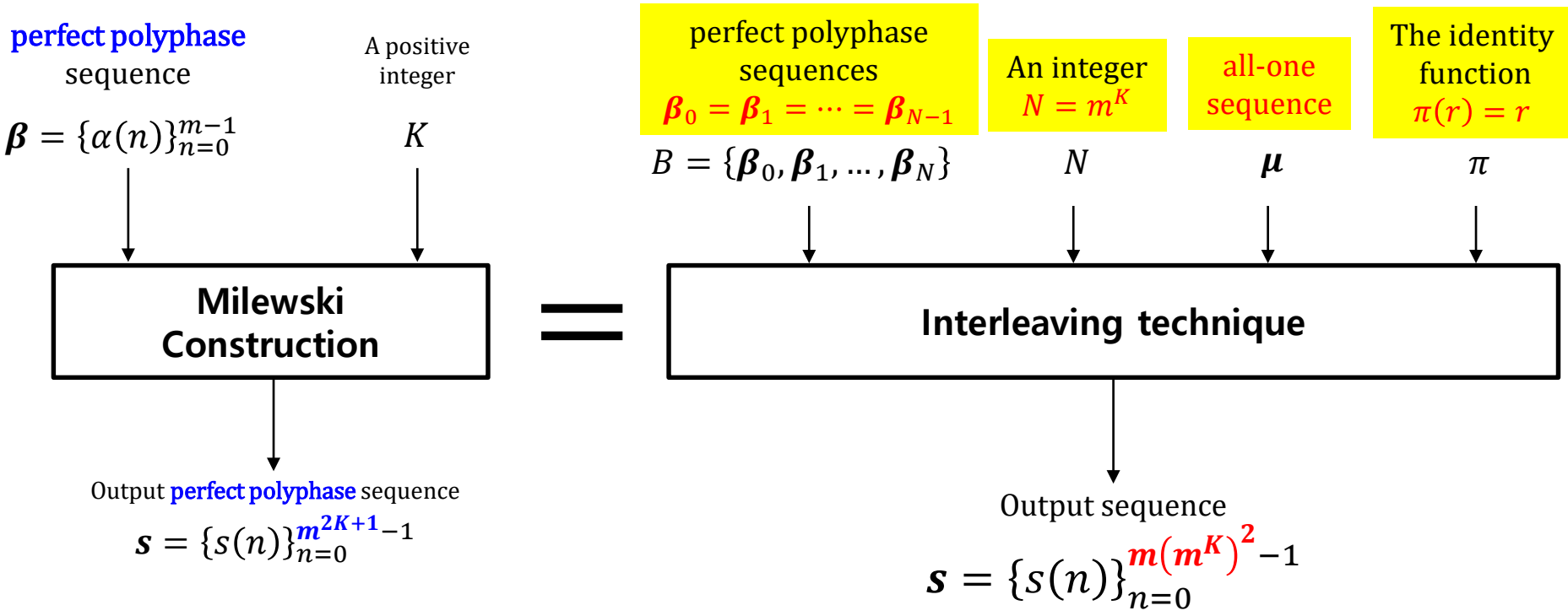
Milewski Construction is a Special Case



where

$$s(n) = \beta(q)\omega^{q\boldsymbol{r}}$$

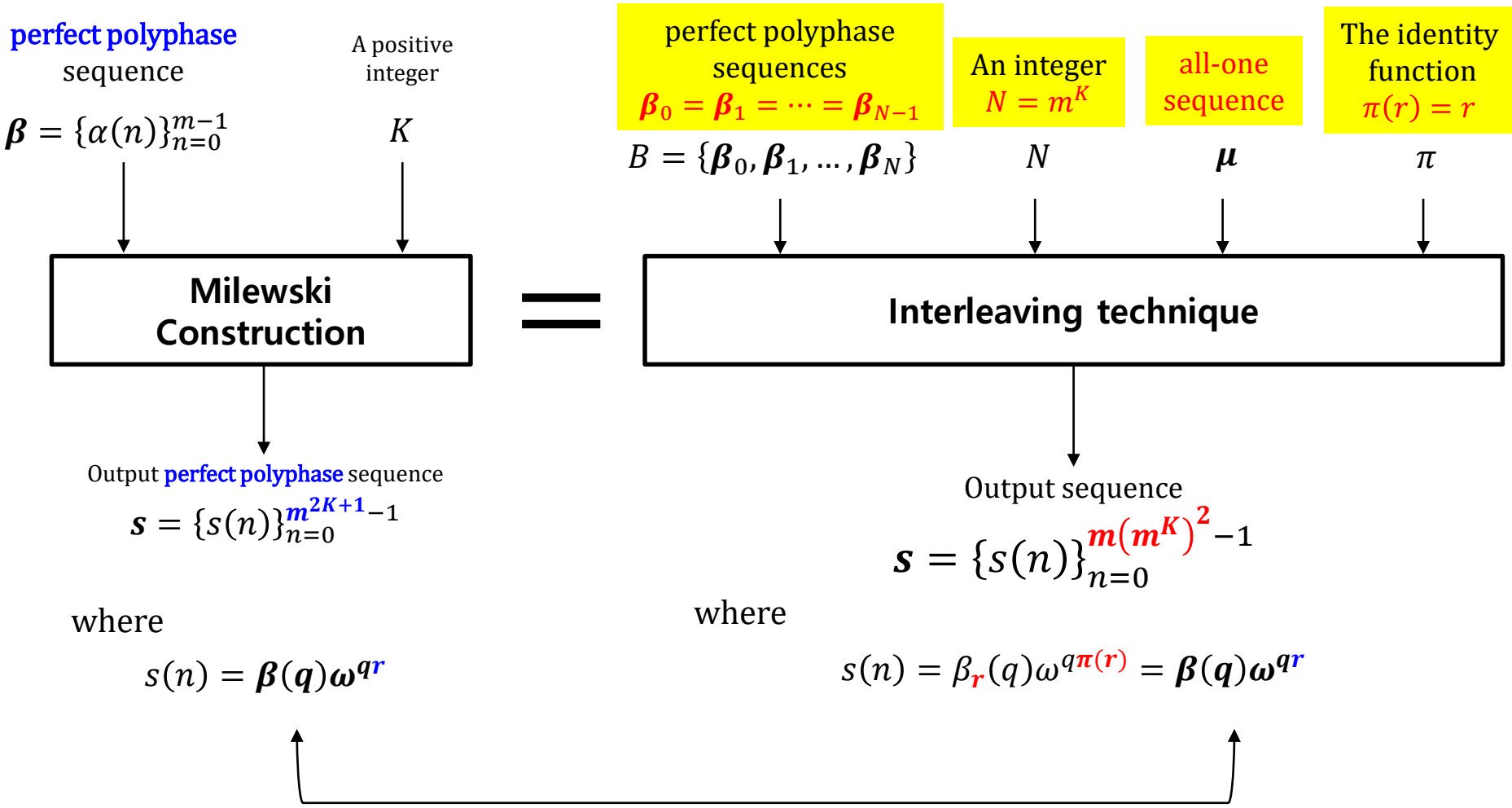
Milewski Construction is a Special Case



where

$$s(n) = \beta(q)\omega^{qr}$$

Milewski Construction is a Special Case



Important Link

Definition. Let $\boldsymbol{\pi}, \boldsymbol{\sigma}$ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$. We define

$$\boldsymbol{\Psi_{\pi,\sigma}(\tau) = \{ x \in \mathbb{Z}_N | \pi(x+\tau) \equiv \sigma(x) \pmod{N} \}.}$$

When $\boldsymbol{\pi = \sigma}$, we use $\boldsymbol{\Psi_{\pi}(\tau)}$ simply.

Condition on perfectness
(Main result 1)

Definition. Let $\boldsymbol{\pi}, \boldsymbol{\sigma}$ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$. We define

$$\boldsymbol{\Psi_{\pi,\sigma}(\tau) = \{ x \in \mathbb{Z}_N | \pi(x+\tau) \equiv \sigma(x) \pmod{N} \}.}$$

When $\boldsymbol{\pi = \sigma}$, we use $\boldsymbol{\Psi_{\pi}(\tau)}$ simply.

Theorem. Any sequence in $\boldsymbol{\mathcal{A}(B,\pi)}$ is perfect **if and only if** the following conditions are satisfied:

1) $\boldsymbol{|\Psi_{\pi}(r)| = 0}$ for $\boldsymbol{r = 1, 2, \dots, N-1}$.
That is, $\boldsymbol{\pi(r) \pmod{N}}$ for $\boldsymbol{r = 0, 1, \dots, N-1}$ is a permutation over $\mathbb{Z}_N$.

2) $\boldsymbol{B}$ is a collection of perfect sequences all of period m with the same energy.

Condition on perfectness
(Main result 1)

Definition. Let $\boldsymbol{\pi, \sigma}$ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$. We define

$$\boldsymbol{\Psi_{\pi,\sigma}(\tau) = \{ x \in \mathbb{Z}_N | \pi(x+\tau) \equiv \sigma(x) \pmod N \}.}$$

When $\boldsymbol{\pi = \sigma}$, we use $\boldsymbol{\Psi_\pi(\tau)}$ simply.

Theorem. Any sequence in $\boldsymbol{\mathcal{A}(B, \pi)}$ is perfect **if and only if** the following conditions are satisfied:

1) $\boldsymbol{|\Psi_\pi(r)| = 0}$ for $\boldsymbol{r = 1, 2, \dots, N-1}$.
That is, $\boldsymbol{\pi(r) \pmod N}$ for $\boldsymbol{r = 0, 1, \dots, N-1}$ is a permutation over $\mathbb{Z}_N$.

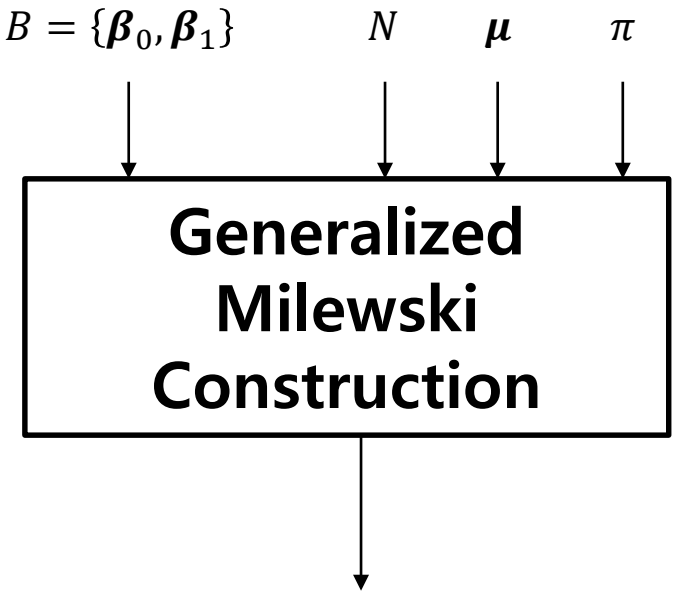
2) $\boldsymbol{B}$ is a collection of perfect sequences all of period m with the same energy.

We now call them

the generalized Milewski sequences

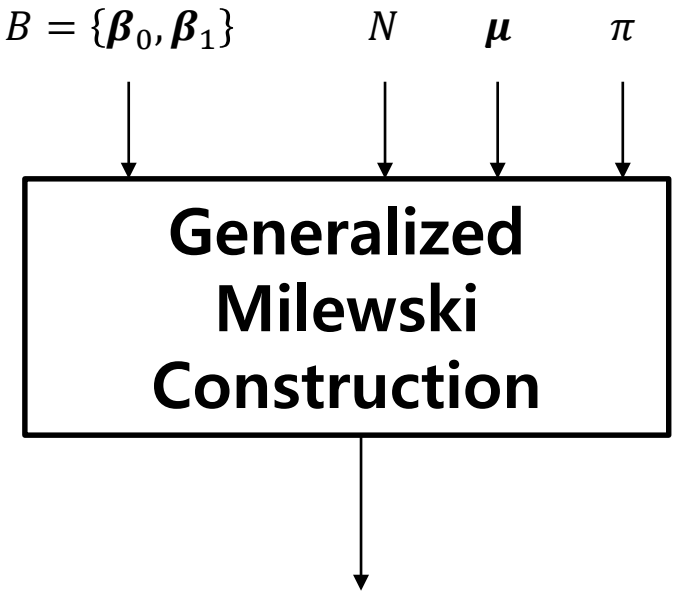
Examples

- $\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \{0, -1, 1, 0, 1, 1\}$
  which is a perfect sequence of length 6,
- $N = 2$,
- $\pi(r) = r$, and
- $\boldsymbol{\mu}$ is the all-one sequence.



Examples

- $\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \{0, -1, 1, 0, 1, 1\}$
  which is a perfect sequence of length 6,
- $N = 2$,
- $\pi(r) = r$, and
- $\boldsymbol{\mu}$ is the all-one sequence.

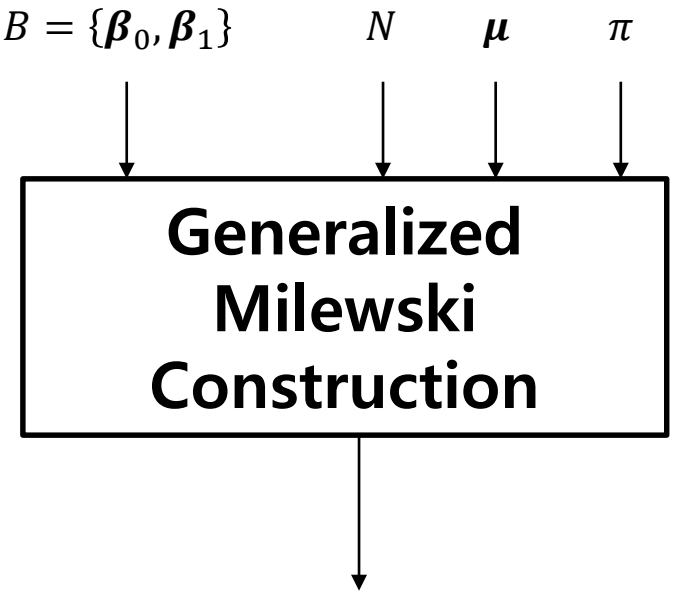


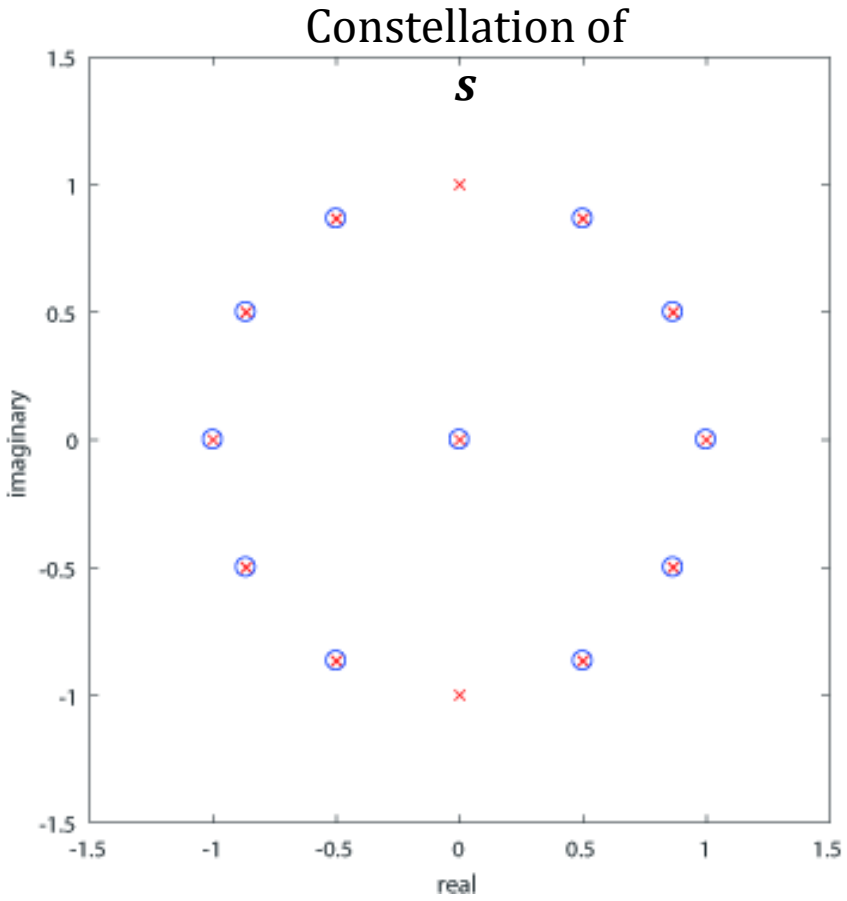
$\boldsymbol{s} = \{0, 0, -1, -\omega, 1, \omega^2, 0, 0, 1, \omega^4, 1, \omega^5, 0, 0, -1, -\omega^7, 1, \omega^8, 0, 0, 1, \omega^{10}, 1, \omega^{11}\}$
is a perfect sequence of length 24.

※ $\omega = e^{-j\frac{2\pi}{12}}$

Examples

- $\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \{0, -1, 1, 0, 1, 1\}$ which is a perfect sequence of length 6,
- $N = 2$,
- $\pi(r) = r$, and
- $\boldsymbol{\mu}$ is the all-one sequence.





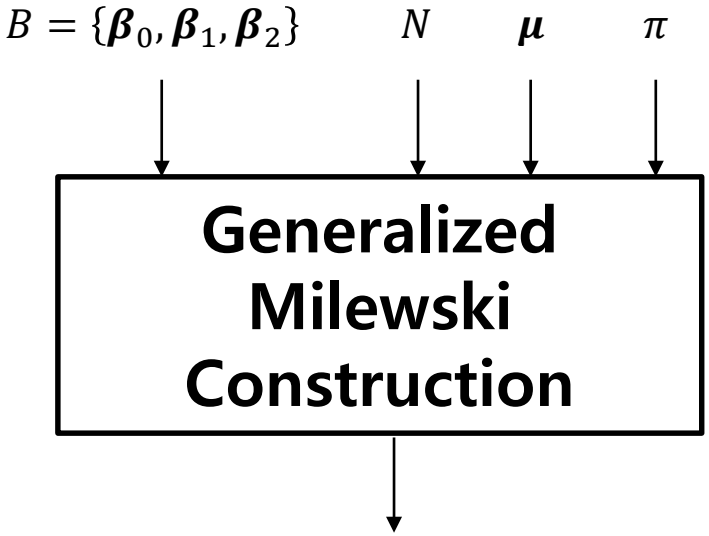
$\boldsymbol{s} = \{0, 0, -1, -\omega, 1, \omega^2, 0, 0, 1, \omega^4, 1, \omega^5, 0, 0, -1, -\omega^7, 1, \omega^8, 0, 0, 1, \omega^{10}, 1, \omega^{11}\}$ is a perfect sequence of length 24.

※ $\omega = e^{-j\frac{2\pi}{12}}$

Examples

ASK constellation

- $\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \boldsymbol{\beta}_2 =$ $\{3, -2, 3, -2, -2, 3, -2, -7, -2, -2\}$ which is a perfect sequence of period 10
- $N = 3$,
- $\pi(r) = r$, and
- $\boldsymbol{\mu}$ is the all-one sequence.



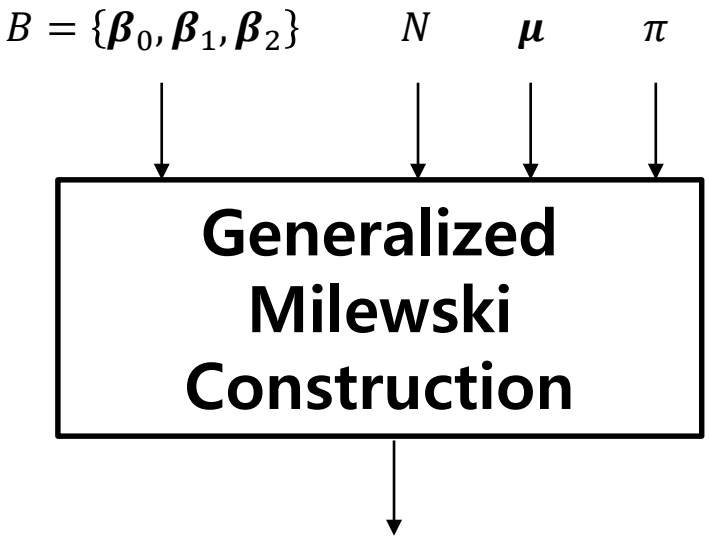
$\boldsymbol{s}$ is a perfect sequence of length 90.

※ $\omega = e^{-j\frac{2\pi}{12}}$

Examples

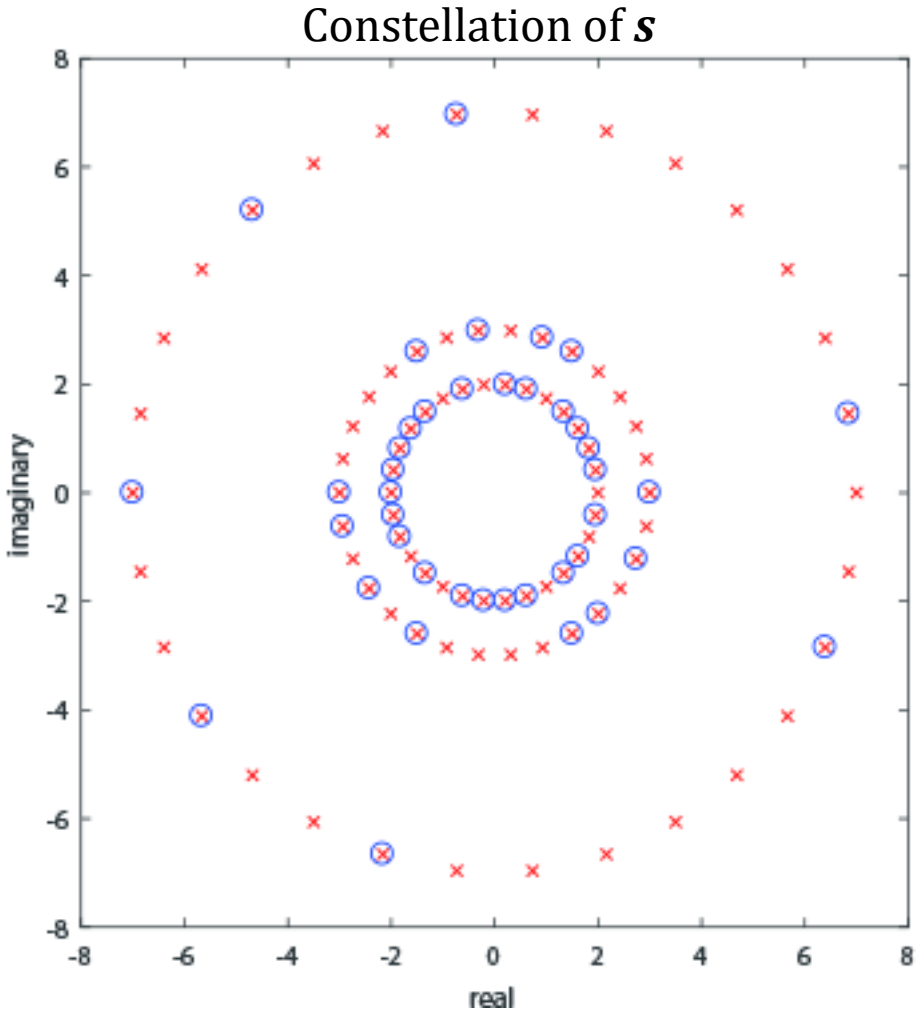
ASK constellation

- $\boldsymbol{\beta}_0 = \boldsymbol{\beta}_1 = \boldsymbol{\beta}_2 = \{3, -2, 3, -2, -2, 3, -2, -7, -2, -2\}$ which is a perfect sequence of period 10
- $N = 3$,
- $\pi(r) = r$, and
- $\boldsymbol{\mu}$ is the all-one sequence.



$\boldsymbol{s}$ is a perfect sequence of length 90.

※ $\omega = e^{-j\frac{2\pi}{12}}$

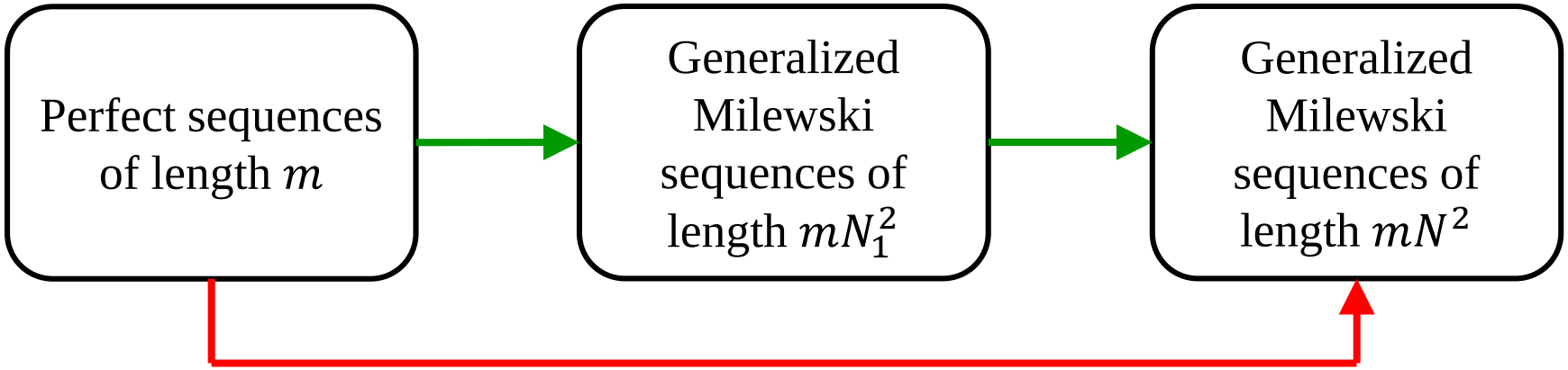


APSK constellation

Direct vs Indirect

(when N is composite)

Two-step synthesis

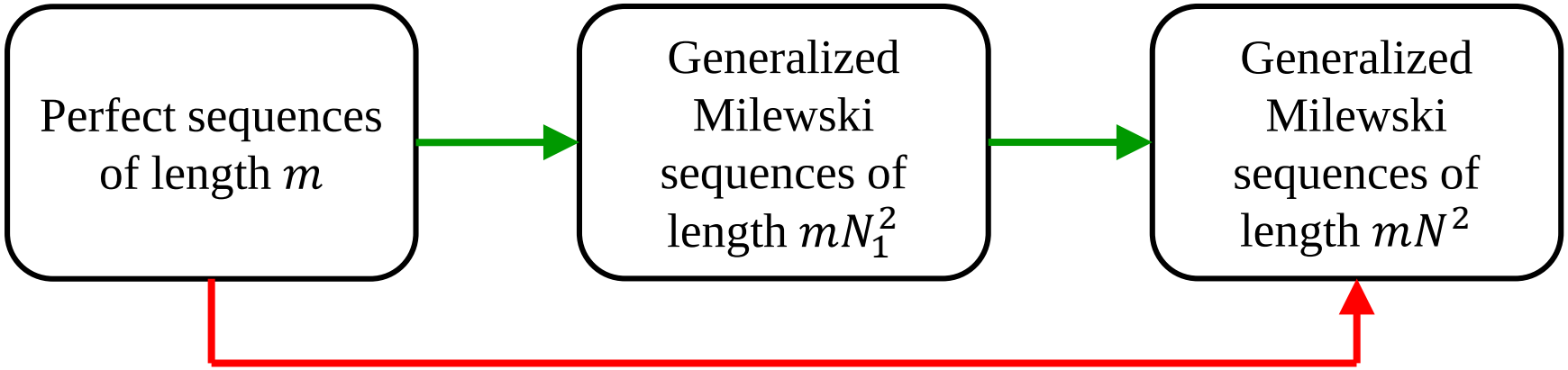


Direct synthesis

Direct vs Indirect

(when N is composite)

Two-step synthesis



Theorem. Assume that N is a composite number.

1) Any generalized Milewski sequence of length mN^2 from the two-step method can be also obtained by the direct method.
2) There exists a generalized Milewski sequence of length mN^2 from the direct method which can not be obtained by the two-step method.

Condition on optimal pair

(Main result 2)

Theorem. Let $B_1 = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \cdots, \boldsymbol{\beta}_{N-1}\}$ and $B_2 = \{\boldsymbol{\gamma}_0, \boldsymbol{\gamma}_1, \cdots, \boldsymbol{\gamma}_{N-1}\}$, all of length m and the same energy E_B, and perfect.

Construct $\boldsymbol{s} \in \boldsymbol{\mathcal{A}}(B_1, \pi)$ and $\boldsymbol{f} \in \boldsymbol{\mathcal{A}}(B_2, \sigma)$.

Condition on optimal pair

(Main result 2)

Theorem. Let $B_1 = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}\}$ and $B_2 = \{\boldsymbol{\gamma}_0, \boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_{N-1}\}$, all of length m and the same energy E_B, and perfect.

Construct $\boldsymbol{s} \in \boldsymbol{\mathcal{A}}(B_1, \pi)$ and $\boldsymbol{f} \in \boldsymbol{\mathcal{A}}(B_2, \sigma)$.

Then, $\boldsymbol{s}$ and $\boldsymbol{f}$ have **optimal crosscorrelation if and only if** the following conditions are satisfied for each $\boldsymbol{r = 0, 1, \ldots, N-1}$:

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.

2) For the unique $x \in \Psi_{\pi,\sigma}(r)$, the pair of sequences

$$\left\{\beta_{x+r}(t)\omega_m^{\pi(x+r)t}\right\}_{t=0}^{m-1} \quad \text{and} \quad \left\{\gamma_x(t)\omega_m^{\sigma(x)t}\right\}_{t=0}^{m-1}$$ is optimal.

Condition on optimal pair

(Simple Special Case)

Corollary. Let $B_1 = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \cdots, \boldsymbol{\beta}_{N-1}\}$ and $B_2 = \{\boldsymbol{\gamma}_0, \boldsymbol{\gamma}_1, \cdots, \boldsymbol{\gamma}_{N-1}\}$, all of length m and the same energy E_B, and perfect.

Assume that $\boldsymbol{\pi}$ and $\boldsymbol{\sigma}$ have the same range.

Construct $\boldsymbol{s} \in \boldsymbol{\mathcal{A}}(B_1, \pi)$ and $\boldsymbol{f} \in \boldsymbol{\mathcal{A}}(B_2, \sigma)$.

Condition on optimal pair
(Simple Special Case)

Corollary. Let $B_1 = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}\}$ and $B_2 = \{\boldsymbol{\gamma}_0, \boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_{N-1}\}$, all of length m and the same energy E_B, and perfect.

Assume that $\boldsymbol{\pi}$ and $\boldsymbol{\sigma}$ have the same range.

Construct $\boldsymbol{s} \in \boldsymbol{\mathcal{A}}(B_1, \pi)$ and $\boldsymbol{f} \in \boldsymbol{\mathcal{A}}(B_2, \sigma)$.

Then, $\boldsymbol{s}$ and $\boldsymbol{f}$ have **optimal crosscorrelation if and only if** the following conditions are satisfied for each $\boldsymbol{r = 0, 1, \ldots, N-1}$:

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.
2) For the unique $x \in \Psi_{\pi,\sigma}(r)$,

the pair of sequences $\boldsymbol{\beta}_{x+r}$ and $\boldsymbol{\gamma}_x$ is optimal.

Condition on optimal pair
(Simple Special Case)

Corollary. Let $B_1 = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}\}$ and $B_2 = \{\boldsymbol{\gamma}_0, \boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_{N-1}\}$, all of length m and the same energy E_B, and perfect.

Assume that $\boldsymbol{\pi}$ and $\boldsymbol{\sigma}$ have the same range.

Construct $\boldsymbol{s} \in \boldsymbol{\mathcal{A}}(B_1, \pi)$ and $\boldsymbol{f} \in \boldsymbol{\mathcal{A}}(B_2, \sigma)$.

Then, $\boldsymbol{s}$ and $\boldsymbol{f}$ have **optimal crosscorrelation if and only if** the following conditions are satisfied for each $\boldsymbol{r = 0, 1, \ldots, N-1}$:

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.

2) For the unique $x \in \Psi_{\pi,\sigma}(r)$,

the pair of sequences $\boldsymbol{\beta}_{x+r}$ and $\boldsymbol{\gamma}_x$ is optimal.

Condition on input pairs

Condition on optimal pair
(Simple Special Case)

Corollary. Let $B_1 = \{\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{N-1}\}$ and $B_2 = \{\boldsymbol{\gamma}_0, \boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_{N-1}\}$, all of length m and the same energy E_B, and perfect.

Assume that $\boldsymbol{\pi}$ and $\boldsymbol{\sigma}$ have the same range.

Construct $\boldsymbol{s} \in \boldsymbol{\mathcal{A}}(B_1, \pi)$ and $\boldsymbol{f} \in \boldsymbol{\mathcal{A}}(B_2, \sigma)$.

Then, $\boldsymbol{s}$ and $\boldsymbol{f}$ have **optimal crosscorrelation if and only if** the following conditions are satisfied for each $\boldsymbol{r = 0, 1, \ldots, N-1}$:

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.

Condition on input permutations

2) For the unique $x \in \Psi_{\pi,\sigma}(r)$,

the pair of sequences $\boldsymbol{\beta}_{x+r}$ and $\boldsymbol{\gamma}_x$ is optimal.

Condition on input pairs

when $m = 1$

- The all-one sequence of length 1 is a trivial perfect sequence.
- Therefore,

> "the all-one sequence and itself is a (trivial) optimal pair of perfect sequences of length 1"

when $m = 1$

- The all-one sequence of length 1 is a trivial perfect sequence.
- Therefore,

> "the all-one sequence and itself is a (trivial) optimal pair of perfect sequences of length 1"

- Therefore, for $m = 1$, we have:

an optimal k-set of **generalized Milewski sequences of length N^2** exists
if and only if
a $k \times N$ **circular Florentine array** exists

Example

- For a 4×15 circular Florentine array (Song, 91 and 00)

π_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
π_2	0	7	1	8	2	12	3	11	9	4	13	5	14	6	10
π_3	0	4	11	7	10	1	13	9	5	8	3	6	2	14	12
π_4	0	13	7	2	11	6	14	10	3	5	12	9	1	4	8

we have **optimal 4-set of generalized Milewski sequences** of length $\boldsymbol{N^2 = 15^2}$ by **picking up any** single perfect sequence from each and every family

$$\mathcal{A}(\{1\}, \pi_1),\ \mathcal{A}(\{1\}, \pi_2),\ \mathcal{A}(\{1\}, \pi_3),\ \text{and}$$

$$\mathcal{A}(\{1\}, \pi_4).$$

Example

- For a $\mathbf{4 \times 15}$ **circular Florentine array** (Song, 91 and 00)

π_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
π_2	0	7	1	8	2	12	3	11	9	4	13	5	14	6	10
π_3	0	4	11	7	10	1	13	9	5	8	3	6	2	14	12
π_4	0	13	7	2	11	6	14	10	3	5	12	9	1	4	8

we have **optimal 4-set of generalized Milewski sequences** of length $\boldsymbol{N^2 = 15^2}$ by **picking up any** single perfect sequence from each and every family

$$\mathcal{A}(\{1\}, \pi_1),\ \mathcal{A}(\{1\}, \pi_2),\ \mathcal{A}(\{1\}, \pi_3),\ \text{and}$$

$$\mathcal{A}(\{1\}, \pi_4)$$

- New, in the sense of size **4** (previously known only of size **2**) for length $\mathbf{15^2}$ or **15**

when $m > 1$

Assume we have an optimal pair $\boldsymbol{\beta}, \boldsymbol{\gamma}$ and **a 2×5 circular Florentine array:**

π_1	0	1	2	3	4
π_2	0	2	4	1	3

when $m > 1$

Assume we have an optimal pair $\boldsymbol{\beta}, \boldsymbol{\gamma}$ and **a 2×5 circular Florentine array:**

π_1	0	1	2	3	4
π_2	0	2	4	1	3

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.
2) For the unique $x \in \Psi_{\pi,\sigma}(r)$, the pair of sequences $\boldsymbol{\beta}_{x+r}$ and $\boldsymbol{\gamma}_x$ is optimal.

when $m > 1$

Assume we have an optimal pair $\boldsymbol{\beta}, \boldsymbol{\gamma}$ and **a 2×5 circular Florentine array:**

π_1	0	1	2	3	4
π_2	0	2	4	1	3

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.
2) For the unique $x \in \Psi_{\pi,\sigma}(r)$, the pair of sequences $\boldsymbol{\beta}_{x+r}$ and $\boldsymbol{\gamma}_x$ is optimal.

- Construct $s \in \mathcal{A}(B_1, \pi_1)$, $f \in \mathcal{A}(B_2, \pi_2)$ with $B_1 = \{\beta_0, \beta_1, \ldots, \beta_{N-1}\}$ and $B_2 = \{\gamma_0, \gamma_1, \ldots, \gamma_{N-1}\}$, where

$$\boldsymbol{\beta}_0 = \boldsymbol{\beta} \qquad \boldsymbol{\gamma}_0 = \boldsymbol{\gamma}$$
$$\boldsymbol{\beta}_1 = \boldsymbol{\beta} \qquad \boldsymbol{\gamma}_1 = \boldsymbol{\gamma}$$
$$\vdots \qquad\qquad \vdots$$
$$\boldsymbol{\beta}_4 = \boldsymbol{\beta} \qquad \boldsymbol{\gamma}_4 = \boldsymbol{\gamma}$$

when $m > 1$

Assume we have an optimal pair $\boldsymbol{\beta}, \boldsymbol{\gamma}$ and **a 2×5 circular Florentine array:**

π_1	0	1	2	3	4
π_2	0	2	4	1	3

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.
2) For the unique $x \in \Psi_{\pi,\sigma}(r)$, the pair of sequences $\boldsymbol{\beta}_{x+r}$ and $\boldsymbol{\gamma}_x$ is optimal.

- Construct $s \in \mathcal{A}(B_1, \pi_1)$, $f \in \mathcal{A}(B_2, \pi_2)$ with $B_1 = \{\beta_0, \beta_1, \cdots, \beta_{N-1}\}$ and $B_2 = \{\gamma_0, \gamma_1, \cdots, \gamma_{N-1}\}$, where

$$\boldsymbol{\beta}_0 = \boldsymbol{\beta}$$
$$\boldsymbol{\beta}_1 = \boldsymbol{\beta}$$
$$\vdots$$
$$\boldsymbol{\beta}_4 = \boldsymbol{\beta}$$

$$\boldsymbol{\gamma}_0 = \boldsymbol{\gamma}$$
$$\boldsymbol{\gamma}_1 = \boldsymbol{\gamma}$$
$$\vdots$$
$$\boldsymbol{\gamma}_4 = \boldsymbol{\gamma}$$

Then, **any** $s \in \mathcal{A}(B_1, \pi_1)$ and $f \in \mathcal{A}(B_2, \pi_2)$ is an **optimal pair**

when $m > 1$

Assume we have an optimal pair $\boldsymbol{\beta}, \boldsymbol{\gamma}$ and **a 2×5 circular Florentine array:**

π_1	0	1	2	3	4
π_2	0	2	4	1	3

1) $\left|\Psi_{\pi,\sigma}(r)\right| = 1$, i.e., $\Psi_{\pi,\sigma}(r) = \{x\}$.
2) For the unique $x \in \Psi_{\pi,\sigma}(r)$, the pair of sequences $\boldsymbol{\beta}_{x+r}$ and $\boldsymbol{\gamma}_x$ is optimal.

- Construct $s \in \mathcal{A}(B_1, \pi_1)$, $f \in \mathcal{A}(B_2, \pi_2)$ with $B_1 = \{\beta_0, \beta_1, \cdots, \beta_{N-1}\}$ and $B_2 = \{\gamma_0, \gamma_1, \cdots, \gamma_{N-1}\}$, where

$$\boldsymbol{\beta}_0 = \boldsymbol{\gamma} \qquad \boldsymbol{\gamma}_0 = \boldsymbol{\beta}$$
$$\boldsymbol{\beta}_1 = \boldsymbol{\beta} \qquad \boldsymbol{\gamma}_1 = \boldsymbol{\gamma}$$
$$\vdots \qquad\qquad \vdots$$
$$\boldsymbol{\beta}_4 = \boldsymbol{\beta} \qquad \boldsymbol{\gamma}_4 = \boldsymbol{\gamma}$$

Then, **any** $s \in \mathcal{A}(B_1, \pi_1)$ and $f \in \mathcal{A}(B_2, \pi_2)$ is an **optimal pair**

Definition. Let $\boldsymbol{\pi, \sigma}$ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$.

$$\boldsymbol{\Psi_{\pi,\sigma}(r) = \{ x \in \mathbb{Z}_N | \pi(x + r) \equiv \sigma(x) \ (mod\ N) \}.}$$

π_1	0	1	2	3	4
π_2	0	2	4	1	3

$\boldsymbol{\Psi_{1,2}(r) = \{ x \in \mathbb{Z}_N | \pi_1(x + r) \equiv \pi_2(x) \ (mod\ 5) \}}$ $\leftrightarrow$ $\boldsymbol{\beta_{x+r}}$ **and** $\boldsymbol{\gamma_x}$

Definition. Let $\boldsymbol{\pi, \sigma}$ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$.

$$\boldsymbol{\Psi_{\pi,\sigma}(r) = \{ x \in \mathbb{Z}_N | \pi(x + r) \equiv \sigma(x) \pmod{N} \}.}$$

π_1	0	1	2	3	4
π_2	0	2	4	1	3

$$\boldsymbol{\Psi_{1,2}(r) = \{ x \in \mathbb{Z}_N | \pi_1(x + r) \equiv \pi_2(x) \pmod{5} \} \leftrightarrow \beta_{x+r} \text{ and } \gamma_x}$$

$$\Psi_{1,2}(\mathbf{0}) = \{ x \in \mathbb{Z}_N | \pi_1(x + \mathbf{0}) \equiv \pi_2(x) \pmod{5} \} = \{0\} \leftrightarrow \beta_{0+\mathbf{0}} = \beta_{\mathbf{0}} \text{ and } \gamma_{\mathbf{0}}$$
$$\Psi_{1,2}(\mathbf{1}) = \{ x \in \mathbb{Z}_N | \pi_1(x + \mathbf{1}) \equiv \pi_2(x) \pmod{5} \} = \{2\} \leftrightarrow \beta_{2+\mathbf{1}} = \beta_{\mathbf{3}} \text{ and } \gamma_{\mathbf{2}}$$
$$\Psi_{1,2}(\mathbf{2}) = \{ x \in \mathbb{Z}_N | \pi_1(x + \mathbf{2}) \equiv \pi_2(x) \pmod{5} \} = \{4\} \leftrightarrow \beta_{4+\mathbf{2}} = \beta_{\mathbf{1}} \text{ and } \gamma_{\mathbf{4}}$$
$$\Psi_{1,2}(\mathbf{3}) = \{ x \in \mathbb{Z}_N | \pi_1(x + \mathbf{3}) \equiv \pi_2(x) \pmod{5} \} = \{1\} \leftrightarrow \beta_{1+\mathbf{3}} = \beta_{\mathbf{4}} \text{ and } \gamma_{\mathbf{1}}$$
$$\Psi_{1,2}(\mathbf{4}) = \{ x \in \mathbb{Z}_N | \pi_1(x + \mathbf{4}) \equiv \pi_2(x) \pmod{5} \} = \{3\} \leftrightarrow \beta_{3+\mathbf{4}} = \beta_{\mathbf{2}} \text{ and } \gamma_{\mathbf{3}}$$

Definition. Let π, σ be two functions from $\mathbb{Z}_N$ to $\mathbb{Z}_{mN}$.

$$\Psi_{\pi,\sigma}(r) = \{ x \in \mathbb{Z}_N | \pi(x+r) \equiv \sigma(x) \pmod{N} \}.$$

π_1	0	1	2	3	4
π_2	0	2	4	1	3

$$\Psi_{1,2}(r) = \{ x \in \mathbb{Z}_N | \pi_1(x+r) \equiv \pi_2(x) \pmod{5} \} \leftrightarrow \beta_{x+r} \text{ and } \gamma_x$$

$$\Psi_{1,2}(0) = \{ x \in \mathbb{Z}_N | \pi_1(x+0) \equiv \pi_2(x) \pmod{5} \} = \{0\} \leftrightarrow \beta_{0+0} = \beta_0 \text{ and } \gamma_0$$
$$\Psi_{1,2}(1) = \{ x \in \mathbb{Z}_N | \pi_1(x+1) \equiv \pi_2(x) \pmod{5} \} = \{2\} \leftrightarrow \beta_{2+1} = \beta_3 \text{ and } \gamma_2$$
$$\Psi_{1,2}(2) = \{ x \in \mathbb{Z}_N | \pi_1(x+2) \equiv \pi_2(x) \pmod{5} \} = \{4\} \leftrightarrow \beta_{4+2} = \beta_1 \text{ and } \gamma_4$$
$$\Psi_{1,2}(3) = \{ x \in \mathbb{Z}_N | \pi_1(x+3) \equiv \pi_2(x) \pmod{5} \} = \{1\} \leftrightarrow \beta_{1+3} = \beta_4 \text{ and } \gamma_1$$
$$\Psi_{1,2}(4) = \{ x \in \mathbb{Z}_N | \pi_1(x+4) \equiv \pi_2(x) \pmod{5} \} = \{3\} \leftrightarrow \beta_{3+4} = \beta_2 \text{ and } \gamma_3$$

$$(\beta_0 \ \gamma_0) = (\beta, \gamma) \text{ or } (\gamma, \beta)$$
$$(\beta_1 \ \gamma_4) = (\beta, \gamma) \text{ or } (\gamma, \beta)$$
$$(\beta_2 \ \gamma_3) = (\beta, \gamma) \text{ or } (\gamma, \beta)$$
$$(\beta_3 \ \gamma_2) = (\beta, \gamma) \text{ or } (\gamma, \beta)$$
$$(\beta_4 \ \gamma_1) = (\beta, \gamma) \text{ or } (\gamma, \beta)$$

Maximum set size

- Let $\boldsymbol{F_c(N)}$ be the maximum such that an $\boldsymbol{F_c(N) \times N}$ **circular Florentine array** exists.
- Let $\boldsymbol{O_G(mN^2)}$ be the maximum such that an optimal $\boldsymbol{O_G(mN^2)}$**-set** of **generalized Milewski sequences** of length $\boldsymbol{mN^2}$ from perfect sequences of length $\boldsymbol{m}$.

Maximum set size

- Let $\boldsymbol{F_c(N)}$ be the maximum such that an $\boldsymbol{F_c(N) \times N}$ **circular Florentine array** exists.
- Let $\boldsymbol{O_G(mN^2)}$ be the maximum such that an optimal $\boldsymbol{O_G(mN^2)}$**-set** of **generalized Milewski sequences** of length $\boldsymbol{mN^2}$ from perfect sequences of length $\boldsymbol{m}$.

1) When $m = 1$,

$$O_G(\mathrm{mN}^2) = O_G(\mathrm{N}^2) = F_c(N).$$

Maximum set size

- Let $\boldsymbol{F_c(N)}$ be the maximum such that an $\boldsymbol{F_c(N) \times N}$ **circular Florentine array** exists.
- Let $\boldsymbol{O_G(mN^2)}$ be the maximum such that an optimal $\boldsymbol{O_G(mN^2)}$**-set** of **generalized Milewski sequences** of length $\boldsymbol{mN^2}$ from perfect sequences of length $\boldsymbol{m}$.

1) When $m = 1$,

$$O_G(\mathrm{mN}^2) = O_G(\mathrm{N}^2) = F_c(N).$$

2) When $m \geq 2$,

$$O_G(\mathrm{mN}^2) = \min\{O_P(m), F_c(N)\}$$

where $O_P(m)$ is the maximum such that an optimal $O_P(m)$-set of perfect sequences of period m.

Concluding remarks

- To obtain an **optimal k-set of generalized Milewski sequences** of length mN^2, we need both:
  - A $k \times N$ **circular Florentine array**, and
  - An **optimal k-set** of **perfect sequences** of length m.

    (When $m = 1$, a trivial example will work always)

Concluding remarks

- To obtain an **optimal k-set of generalized Milewski sequences** of length mN^2, we need both:
  - A $k \times N$ **circular Florentine array**, and
  - An **optimal k-set** of **perfect sequences** of length m.

    (When $m = 1$, a trivial example will work always)

Some open problems:

- Find any other positive odd integer N such that $F_c(N)$ is greater than $p_{min} - 1$.
- Determine the exact value of $F_c(N)$ for every odd N.

Thanks !