Design of Uncorrelated ZCZ Sequences Families from Cyclic Relative Difference Sets

2023 KICS-NA Workshop

Gangsan Kim and Hong-Yeop Song

Channel Coding Lab.

Yonsei University

ZCZ Sequences Family

Definition. (ZCZ Sequences Family)

A set of K sequences of period L:

$$\mathcal{S} = \left\{ \boldsymbol{s}^{(i)} = \left\{ s_t^{(i)} \mid t \in \mathbb{Z}_L \right\} \mid i = 0, 1, \ldots, K-1 \right\}$$

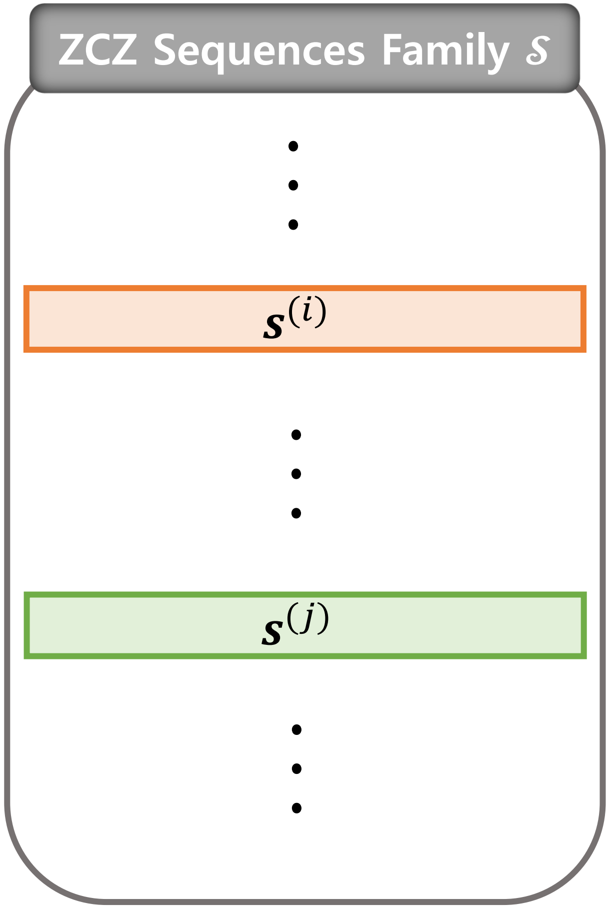
is an (L, K, Z_{cz})-ZCZ sequences family, if

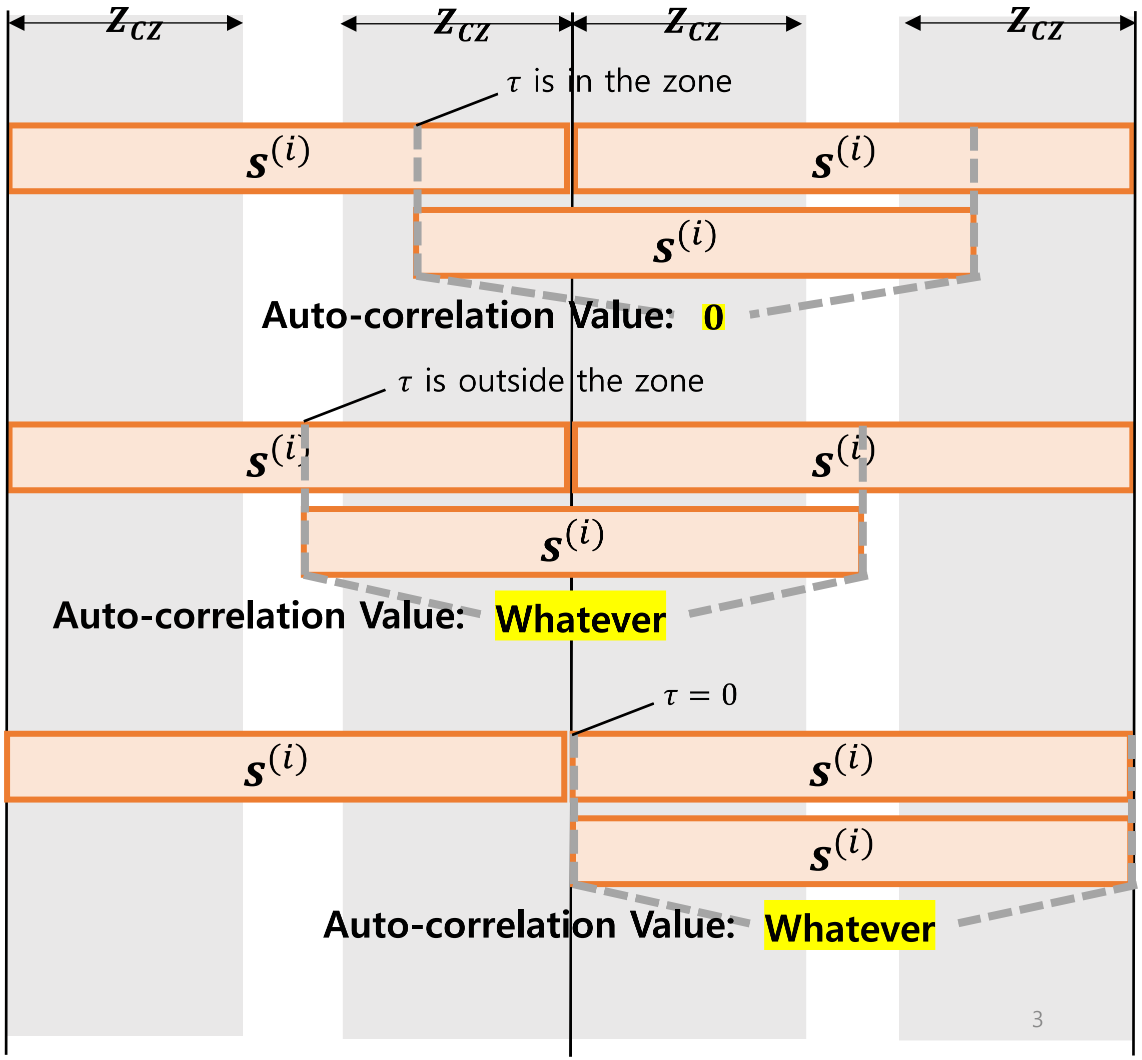
for any i and j, $C_{\boldsymbol{s}^{(i)}, \boldsymbol{s}^{(j)}}(\tau) = 0$ for $|\tau| < Z_{CZ}$,

except for the case of $\tau = 0$ and $i = j$.

Here, Z_{CZ} is called the zero-correlation zone.

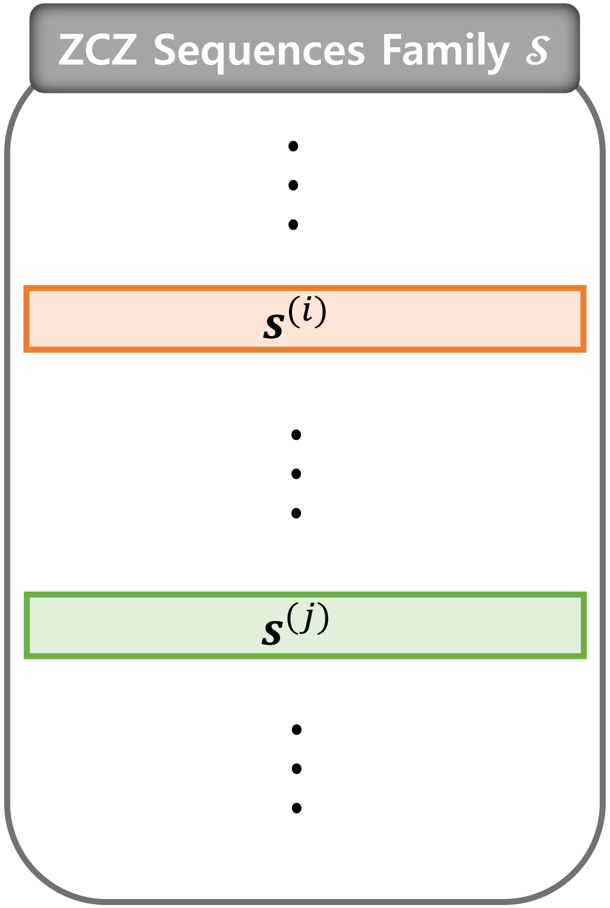
Definition. (ZCZ Sequences Family)

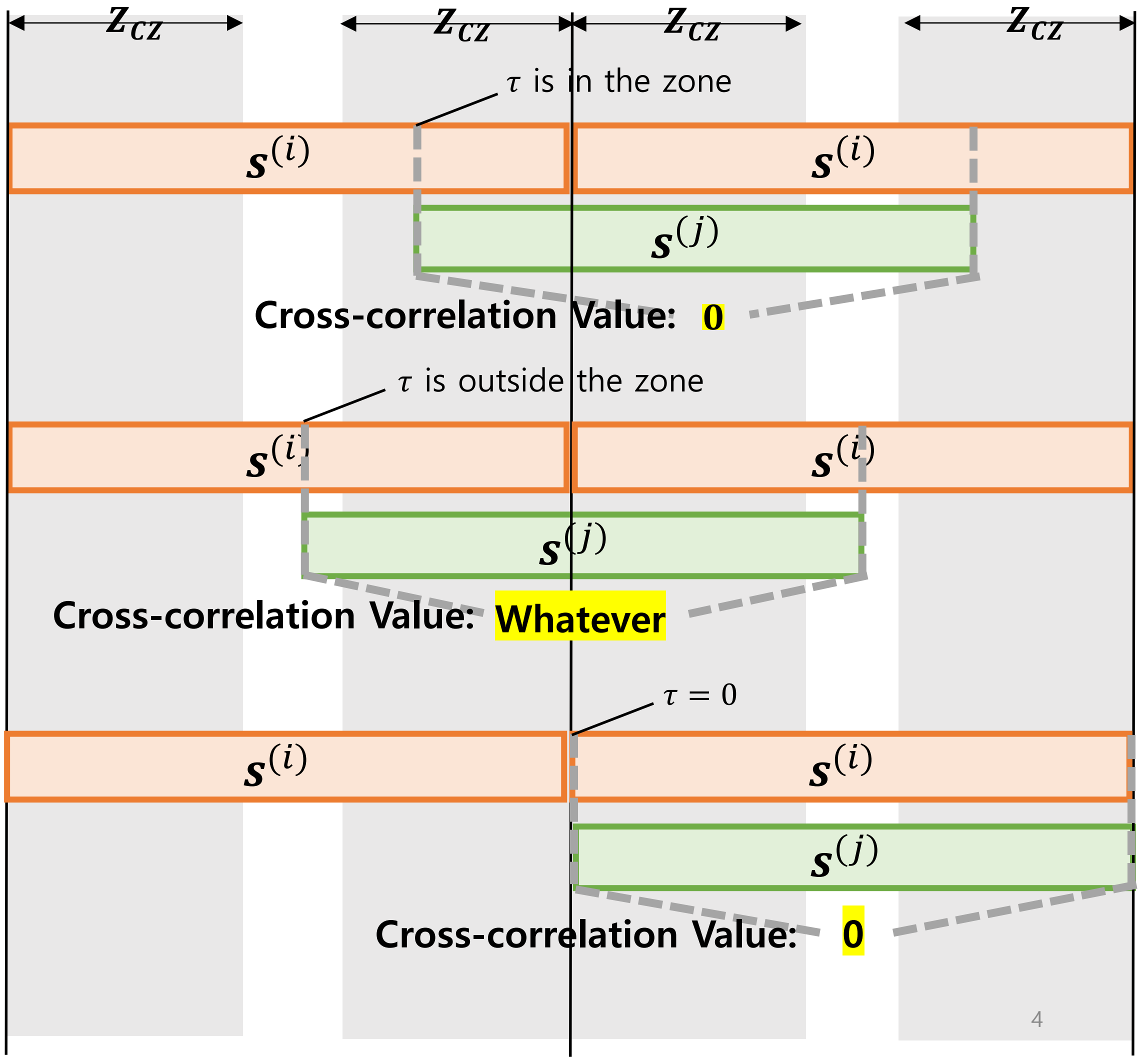




ZCZ Sequences Family

Definition. (ZCZ Sequences Family)





ZCZ Sequences Family

Definition. (ZCZ Sequences Family)

A set of K sequences of period L:

$$\mathcal{S} = \left\{ \boldsymbol{s}^{(i)} = \left\{ s_t^{(i)} \mid t \in \mathbb{Z}_L \right\} \mid i = 0, 1, \dots, K-1 \right\}$$

is an (L, K, Z_{cz})-ZCZ sequences family, if

for any i and j, $C_{\boldsymbol{s}^{(i)}, \boldsymbol{s}^{(j)}}(\tau) = 0$ for $|\tau| < Z_{CZ}$,

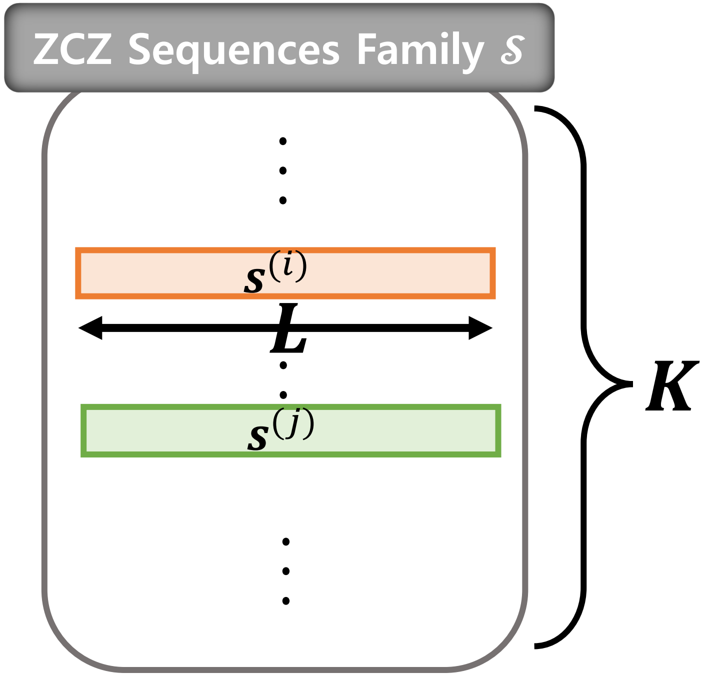
except for the case of $\tau = 0$ and $i = j$.

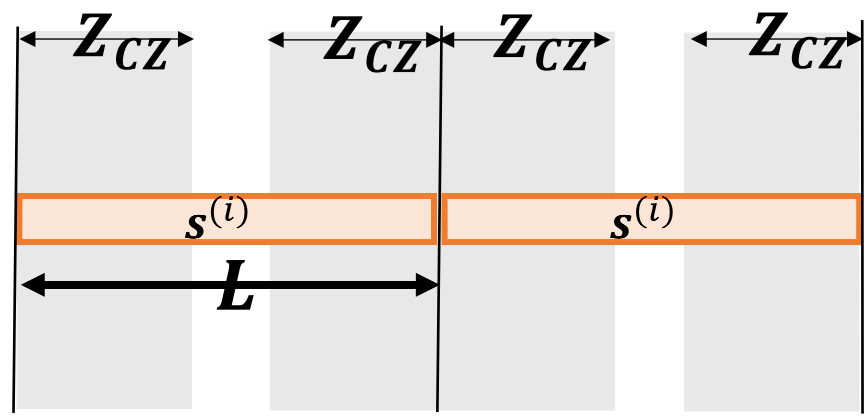
Known Fact 1 (Upper bound [45])

For an (L, K, Z_{cz})-ZCZ sequences family, the size K of the family is upper bounded by

$$K \le L / Z_{cz}$$

ZCZ Sequences Family





Known Fact 1 (Upper bound [45])

For an (L, K, Z_{cz})-ZCZ sequences family, the size K of the family is upper bounded by

$$K \leq L/Z_{cz}$$

Cyclic Relative Difference Sets

Definition 2 (Cyclic Relative Difference Sets)

Let u, v, k, λ be positive integers.
A (u, v, k, λ) relative difference set (RDS) D is
a k-subset $\{d_1, d_2, \dots, d_k\}$ of the integers mod uv
relative to its subgroup $(u) \triangleq u\mathbb{Z}_{uv}$
satisfying the following condition:

$$\Delta_D(d) = \begin{cases} \lambda, & for\ d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv} \\ k, & for\ d = 0 \\ 0, & otherwise. \end{cases}$$

It is called a cyclic RDS since $\mathbb{Z}_{uv}$ is a cyclic (additive) group.

** $\Delta_D(d) \triangleq |(D + d) \cap D|$

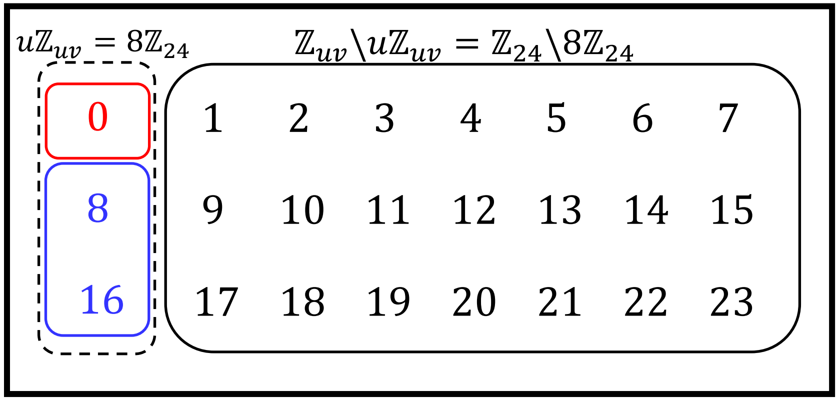
Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

Difference matrix

	0	2	6	7	9	20	21
0	**0**	2	6	7	9	20	21
2	22	**0**	4	5	7	18	19
6	18	20	**0**	1	3	14	15
7	17	19	23	**0**	2	13	14
9	15	17	21	22	**0**	11	12
20	4	6	10	11	13	**0**	1
21	3	5	9	10	12	23	**0**

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$



$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

** $\Delta_D(d) \triangleq |(d + D) \cap D|$

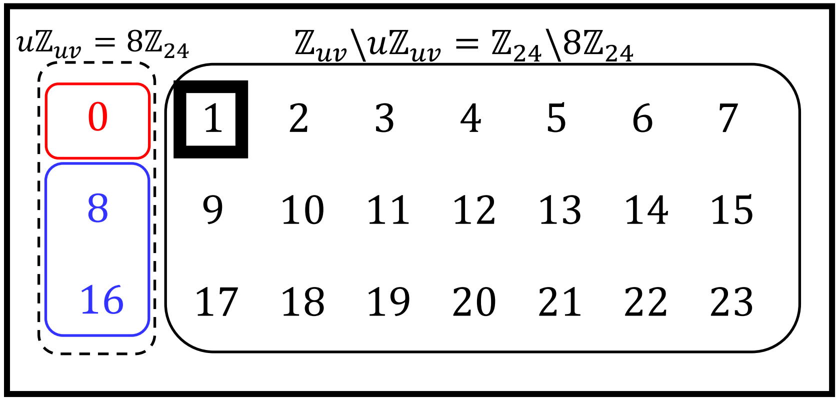
Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0,2,6,7,9,20,21\}$: $(u=8, v=3, k=7, \lambda=2)$-RDS

Difference matrix

	0	2	6	7	9	20	21
0	**0**	2	6	7	9	20	21
2	22	**0**	4	5	7	18	19
6	18	20	**0**	1	3	14	15
7	17	19	23	**0**	2	13	14
9	15	17	21	22	**0**	11	12
20	4	6	10	11	13	**0**	1
21	3	5	9	10	12	23	**0**

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$



$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

** $\Delta_D(d) \triangleq |(d+D) \cap D|$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

Difference matrix

	0	2	6	7	9	20	21
0	**0**	2	6	7	9	20	21
2	22	**0**	4	5	7	18	19
6	18	20	**0**	1	3	14	15
7	17	19	23	**0**	2	13	14
9	15	17	21	22	**0**	11	12
20	4	6	10	11	13	**0**	1
21	3	5	9	10	12	23	**0**

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$u\mathbb{Z}_{uv} = 8\mathbb{Z}_{24}$: 0, 8, 16

$\mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv} = \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$:

1	2	3	4	5	6	7
9	10	11	12	13	14	15
17	18	19	20	21	22	23

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

** $\Delta_D(d) \triangleq |(d + D) \cap D|$

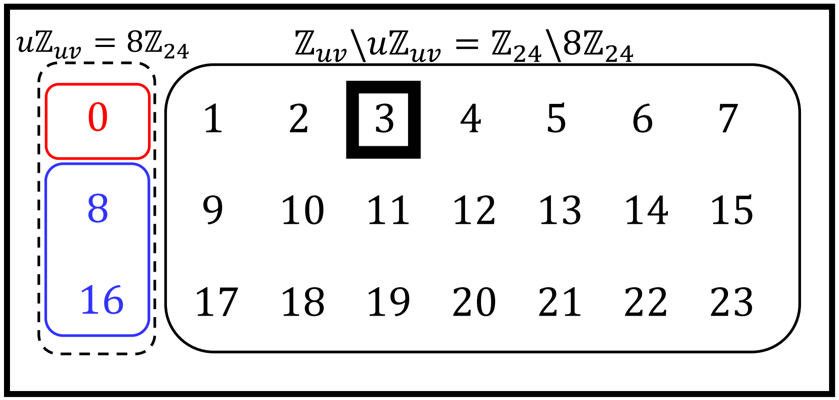
Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

Difference matrix

	0	2	6	7	9	20	21
0	**0**	2	6	7	9	20	21
2	22	**0**	4	5	7	18	19
6	18	20	**0**	1	3	14	15
7	17	19	23	**0**	2	13	14
9	15	17	21	22	**0**	11	12
20	4	6	10	11	13	**0**	1
21	3	5	9	10	12	23	**0**

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$



$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \setminus u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \setminus \{0\}$

** $\Delta_D(d) \triangleq |(d + D) \cap D|$

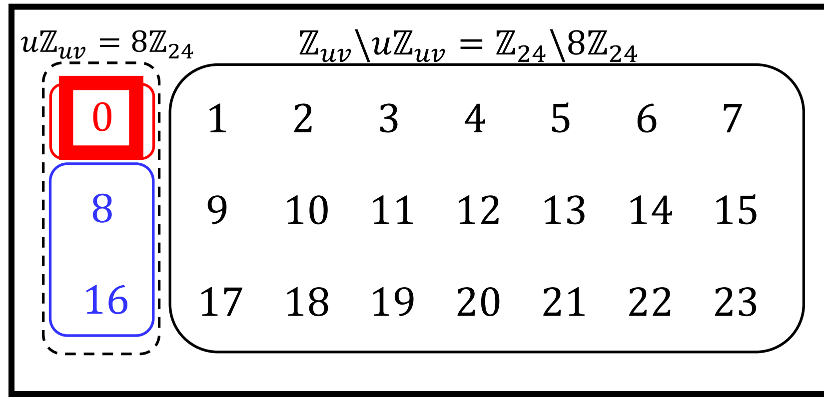
Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

Difference matrix

	0	2	6	7	9	20	21
0	**0**	2	6	7	9	20	21
2	22	**0**	4	5	7	18	19
6	18	20	**0**	1	3	14	15
7	17	19	23	**0**	2	13	14
9	15	17	21	22	**0**	11	12
20	4	6	10	11	13	**0**	1
21	3	5	9	10	12	23	**0**

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$



$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

** $\Delta_D(d) \triangleq |(d + D) \cap D|$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

Difference matrix

	0	2	6	7	9	20	21
0	**0**	2	6	7	9	20	21
2	22	**0**	4	5	7	18	19
6	18	20	**0**	1	3	14	15
7	17	19	23	**0**	2	13	14
9	15	17	21	22	**0**	11	12
20	4	6	10	11	13	**0**	1
21	3	5	9	10	12	23	**0**

No 8

No 16

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$u\mathbb{Z}_{uv} = 8\mathbb{Z}_{24}$: 0, 8, 16

$\mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv} = \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$:

1 2 3 4 5 6 7

9 10 11 12 13 14 15

17 18 19 20 21 22 23

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

** $\Delta_D(d) \triangleq |(d + D) \cap D|$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

Difference matrix

	0	2	6	7	9	20	21
0	**0**	2	6	7	9	20	21
2	22	**0**	4	5	7	18	19
6	18	20	**0**	1	3	14	15
7	17	19	23	**0**	2	13	14
9	15	17	21	22	**0**	11	12
20	4	6	10	11	13	**0**	1
21	3	5	9	10	12	23	**0**

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	10	18	19	20	21	22	23

Example: (8,3,7,2) Cyclic Relative Difference Sets

$\boldsymbol{D = \{0, 2, 6, 7, 9, 20, 21\}}$**:** $\boldsymbol{(u = 8, v = 3, k = 7, \lambda = 2)}$**-RDS**

$$\mathbb{Z}_{\boldsymbol{uv}} = \mathbb{Z}_{\mathbf{24}}$$

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	10	18	19	20	21	22	23

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

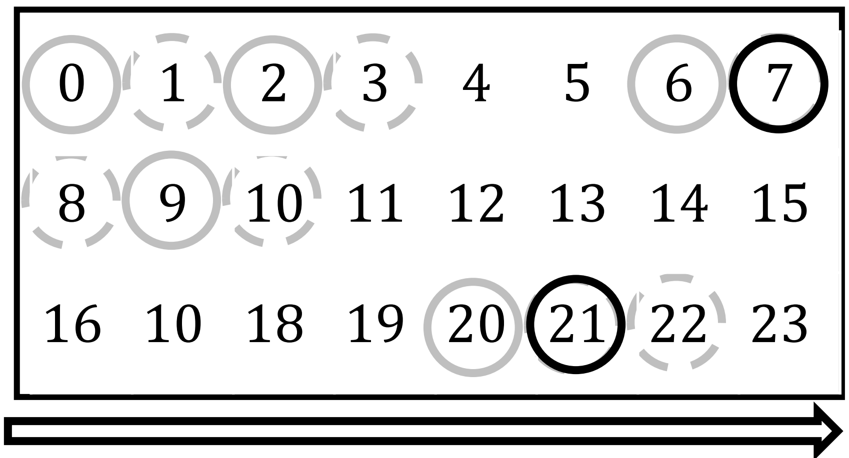
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{\boldsymbol{uv}} \backslash \{\mathbf{0}\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 1$



Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

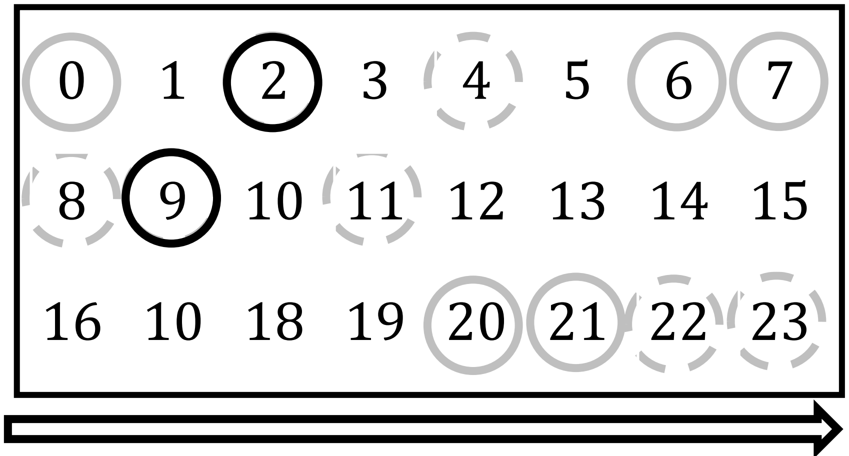
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 2$



Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

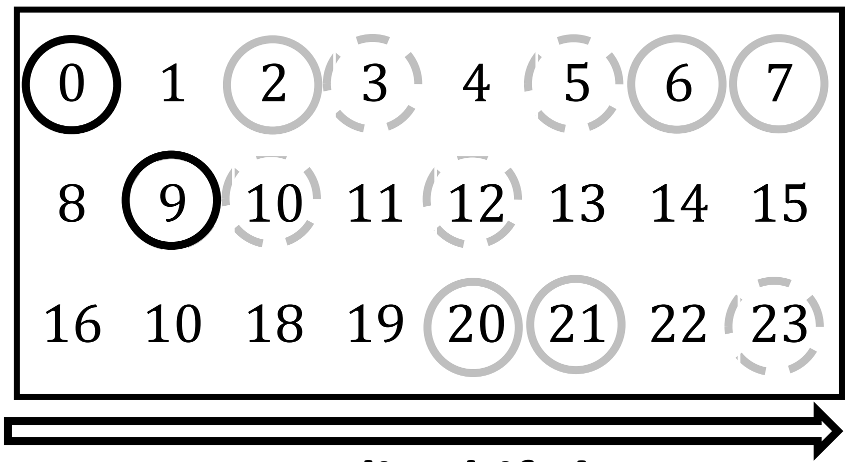
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{\mathbf{0}\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 3$



Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

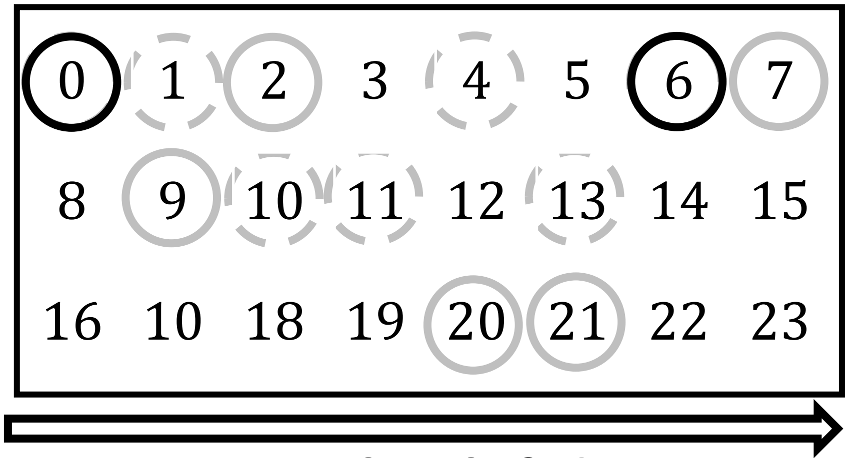
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 4$



Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

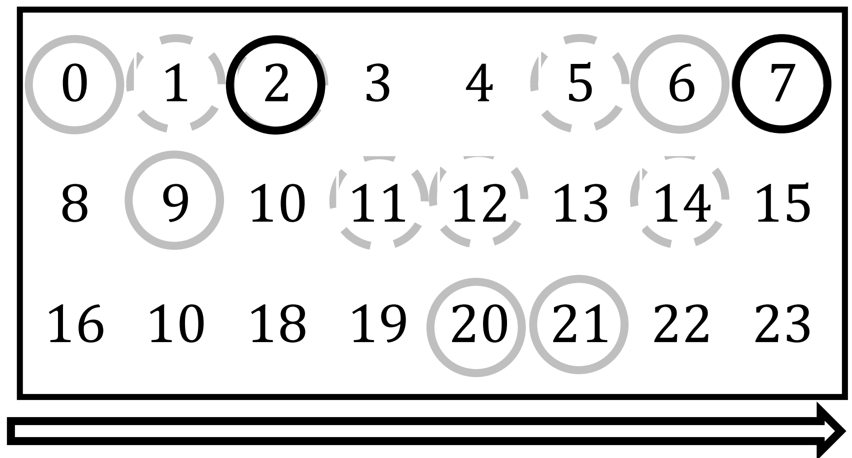
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$\boldsymbol{D} = \{\mathbf{0}, \mathbf{2}, \mathbf{6}, \mathbf{7}, \mathbf{9}, \mathbf{20}, \mathbf{21}\}$: $(\boldsymbol{u} = \mathbf{8}, \boldsymbol{v} = \mathbf{3}, \boldsymbol{k} = \mathbf{7}, \boldsymbol{\lambda} = \mathbf{2})$-**RDS**

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\boldsymbol{\tau} = \mathbf{5}$



Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

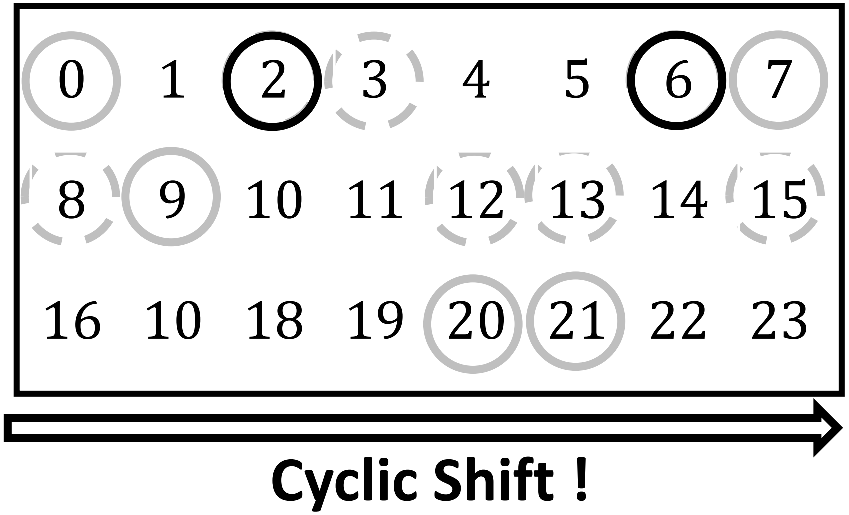
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{\mathbf{0}\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 6$



$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

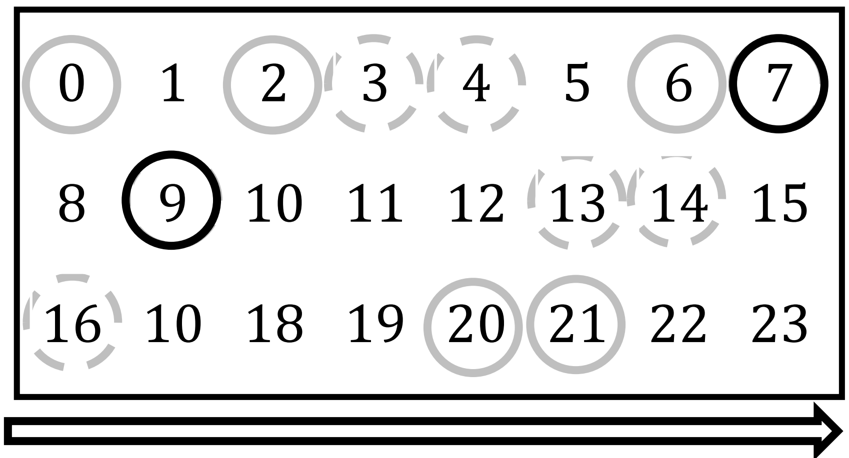
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 7$



Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

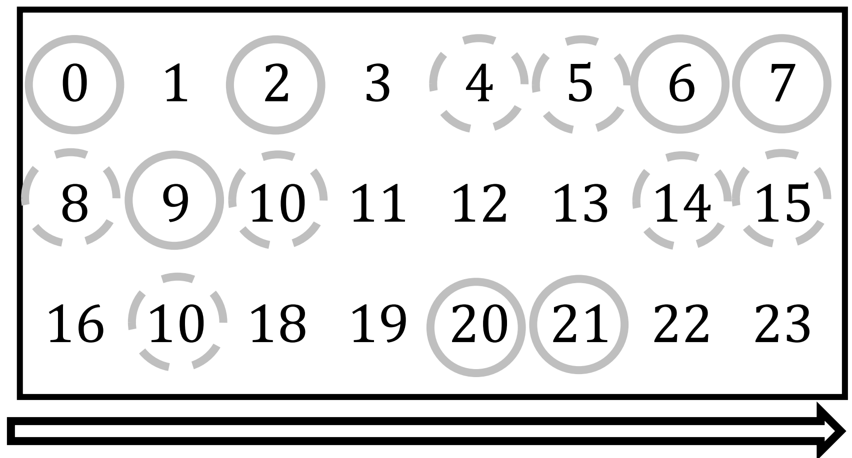
$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 8$



Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 0$

$\tau = 8$

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	10	18	19	20	21	22	23

Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

$\tau = 0$	0	1	2	3	4	5	6	7
$\tau = 8$	8	9	10	11	12	13	14	15
$\tau = 16$	16	10	18	19	20	21	22	23

Cyclic Shift !

$\Delta_D(d) = \lambda = 2$ for $d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}$

$\Delta_D(d) = k = 7$ for $d = 0$

$\Delta_D(d) = 0$ for $d \in u\mathbb{Z}_{uv} \backslash \{0\}$

Example: (8,3,7,2) Cyclic Relative Difference Sets

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\mathbb{Z}_{uv} = \mathbb{Z}_{24}$

				X				
$\tau = 0$	0	1	2	3	4	5	6	7
$\tau = 8$	8	9	10	11	12	13	14	15
$\tau = 16$	16	10	18	19	20	21	22	23

$$\mathbb{Z}_{24} = D \cup (8 + D) \cup (16 + D) \cup X$$

Partition property of cyclic RDS

Proposition 2

Let D be a (u, v, k, λ)-RDS in $\mathbb{Z}_{uv}$ relative to its subgroup $u\mathbb{Z}_{uv}$. Then, we observe the following:

1) The RDS D and all its shifts $iu + D$ for $i = 1, 2, \ldots, v-1$ are **pairwise disjoint**.
2) Let $X \triangleq \mathbb{Z}_{uv} \setminus \cup_{i=0}^{v-1} (iu + D)$ then, X and $iu + D$ for $i = 1, 2, \ldots, v-1$ **partition the group** $\mathbb{Z}_{uv}$. i.e.

$$\mathbb{Z}_{uv} = \left(\bigcup_{i=0}^{v-1} (iu + D) \right) \cup X$$

Characteristic sequence

Proposition 2

Let D be a (u, v, k, λ)-RDS in $\mathbb{Z}_{uv}$ relative to its subgroup $u\mathbb{Z}_{uv}$.
Then, we observe the following:

1) The RDS D and all its shifts $iu + D$ for $i = 1, 2, \ldots, v-1$ are **pairwise disjoint**.
2) Let $X \triangleq \mathbb{Z}_{uv} \setminus \bigcup_{i=0}^{v-1}(iu + D)$ then, X and $iu + D$ for $i = 1, 2, \ldots, v-1$ **partition the group** $\mathbb{Z}_{uv}$. i.e.

$$\mathbb{Z}_{uv} = \left(\bigcup_{i=0}^{v-1}(iu + D)\right) \cup X$$

Definition 3 (Characteristic sequences)

Given sequence $\boldsymbol{a} = \{a_l \mid l \in \mathbb{Z}_v\}$ of length v, we define a sequence $\boldsymbol{s}$ of D associated with $\boldsymbol{a}$ as, for $t = 0, 1, \ldots, uv-1$,

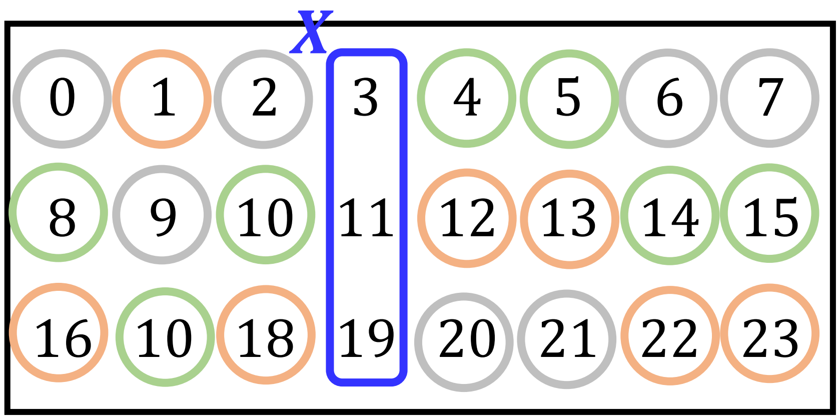
$$s_t = \begin{cases} a_i & \text{if } t \in iu + D \text{ for } 0 \le i < v, \\ 0 & \text{if } t \in X \end{cases}$$

We also call it associated with $(\boldsymbol{a}, D)$.

Characteristic sequence

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$a = \{a_0, a_1, a_2\}$: Sequence of length $v = 3$

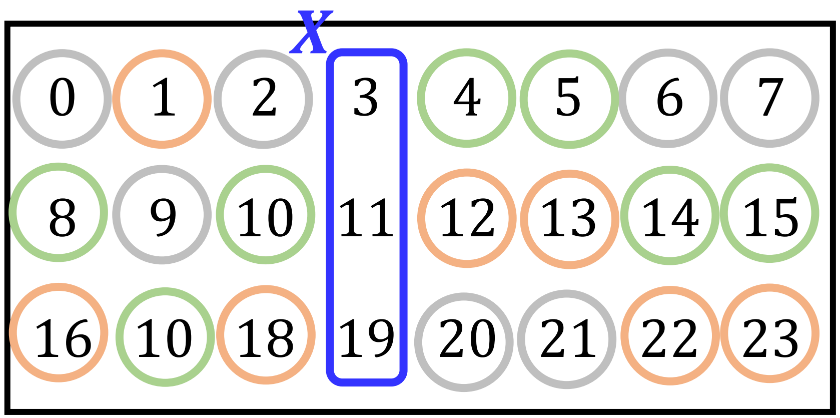


$$\mathbb{Z}_{24} = D \cup (8 + D) \cup (16 + D) \cup X$$

Characteristic sequence

$\boldsymbol{D} = \{\mathbf{0, 2, 6, 7, 9, 20, 21}\}$: $(\boldsymbol{u} = \mathbf{8}, \boldsymbol{v} = \mathbf{3}, \boldsymbol{k} = \mathbf{7}, \boldsymbol{\lambda} = \mathbf{2})$-RDS

$\boldsymbol{a} = \{a_0, a_1, a_2\}$: **Sequence of length** $\boldsymbol{v} = \mathbf{3}$



Substitute! a_0 ⬇ a_1 ⬇ a_2 ⬇ 0 ⬇

$$\mathbb{Z}_{\mathbf{24}} = \boldsymbol{D} \cup (\mathbf{8} + \boldsymbol{D}) \cup (\mathbf{16} + \boldsymbol{D}) \cup \boldsymbol{X}$$

Characteristic sequence

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$a = \{a_0, a_1, a_2\}$: Sequence of length $v = 3$

s_t

$t = 0$	$t = 1$	$t = 2$	$t = 3$	$t = 4$	$t = 5$	$t = 6$	$t = 7$
a_0	a_2	a_0	0	a_1	a_1	a_0	a_0
$t = 8$	$t = 9$	$t = 10$	$t = 11$	$t = 12$	$t = 13$	$t = 14$	$t = 15$
a_1	a_0	a_1	0	a_2	a_2	a_1	a_1
$t = 16$	$t = 17$	$t = 18$	$t = 19$	$t = 20$	$t = 21$	$t = 22$	$t = 23$
a_2	a_1	a_2	0	a_0	a_0	a_2	a_2

Substitute! $a_0 \downarrow$ $a_1 \downarrow$ $a_2 \downarrow$ $0 \downarrow$

$$\mathbb{Z}_{24} = D \cup (8 + D) \cup (16 + D) \cup X$$

S is a sequence associated with (a, D)

Characteristic sequence

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$\boldsymbol{a} = \{a_0, a_1, a_2\}$: Sequence of length $v = 3$

$\boldsymbol{s}$

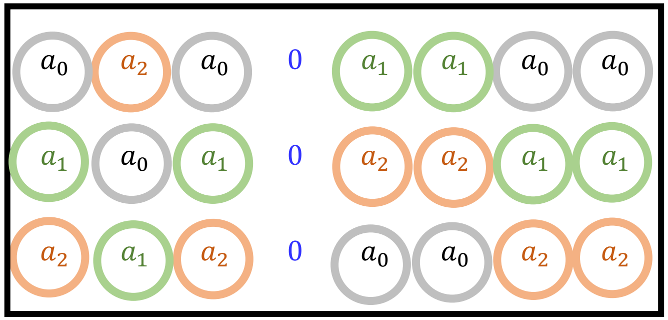
a_0	a_2	a_0	0	a_1	a_1	a_0	a_0
a_1	a_0	a_1	0	a_2	a_2	a_1	a_1
a_2	a_1	a_2	0	a_0	a_0	a_2	a_2

$$\mathbb{Z}_{24} = \boldsymbol{D} \cup (8 + \boldsymbol{D}) \cup (16 + \boldsymbol{D}) \cup \boldsymbol{X}$$

We now want to know the values of autocorrelation of the sequence $\boldsymbol{s}$

Autocorrelation of characteristic sequence

s_t

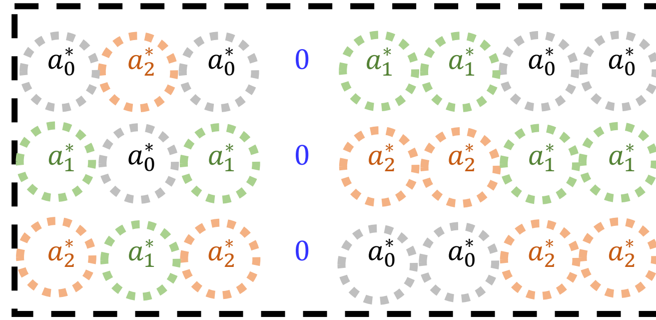


$\boldsymbol{\tau = 0}$

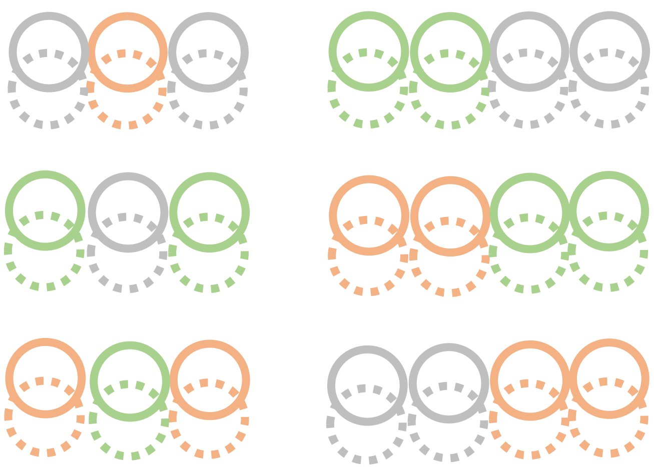
$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$

$s^*_{t-\tau}$



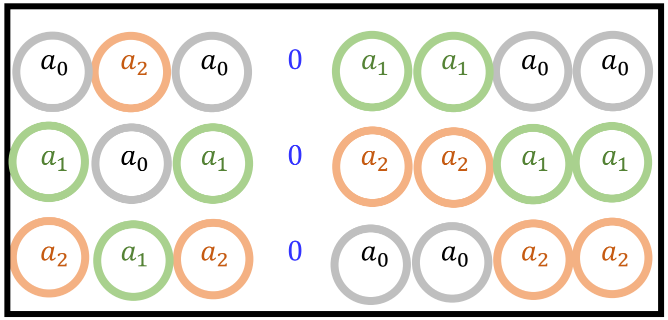
$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$



Autocorrelation of characteristic sequence

$\tau = 0$

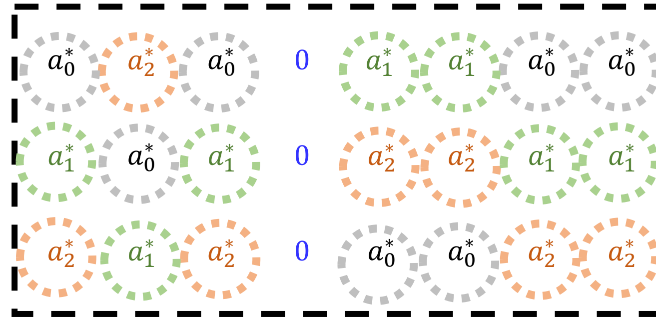
s_t



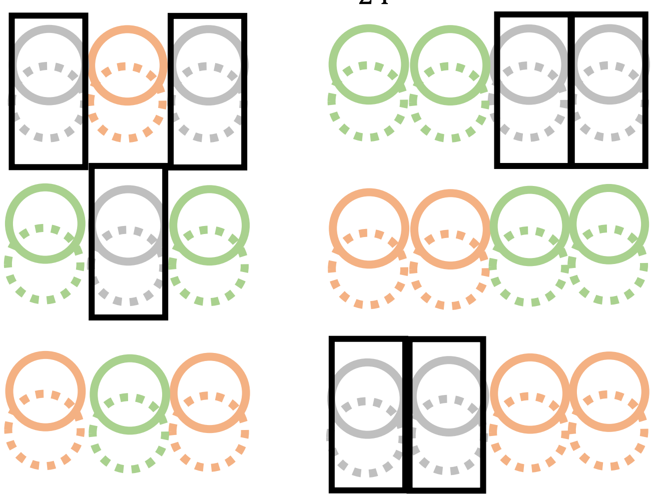
$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$

$s^*_{t-\tau}$



$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$

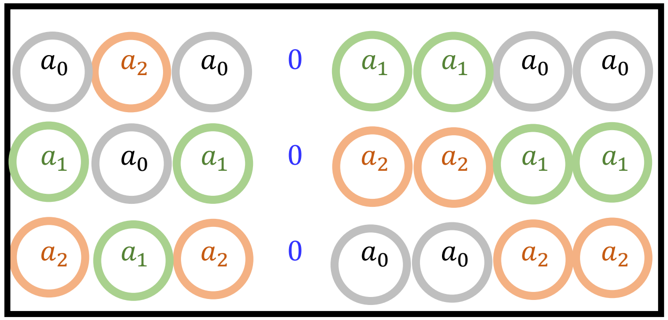


Autocorrelation of characteristic sequence

s_t

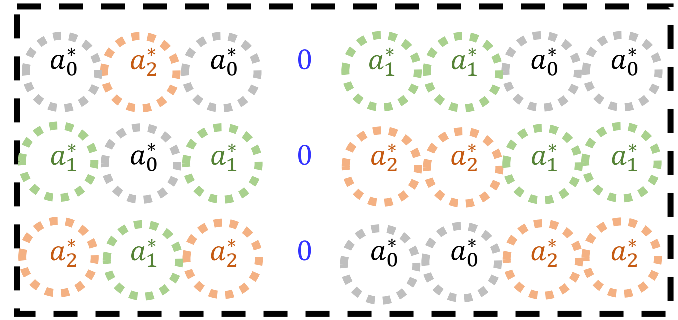
$\boldsymbol{\tau = 0}$

$s^*_{t-\tau}$

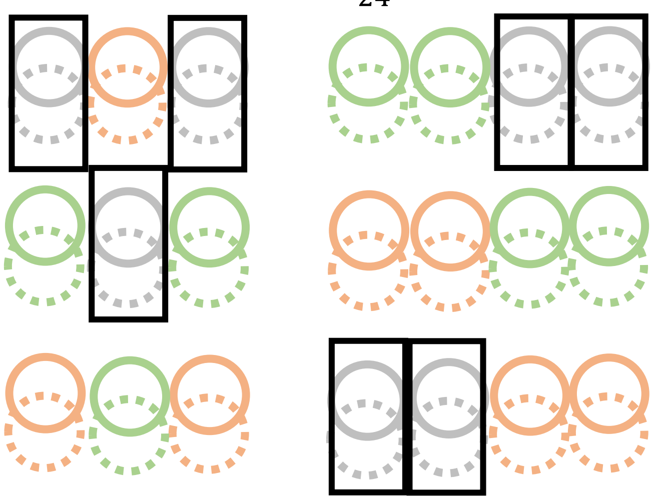


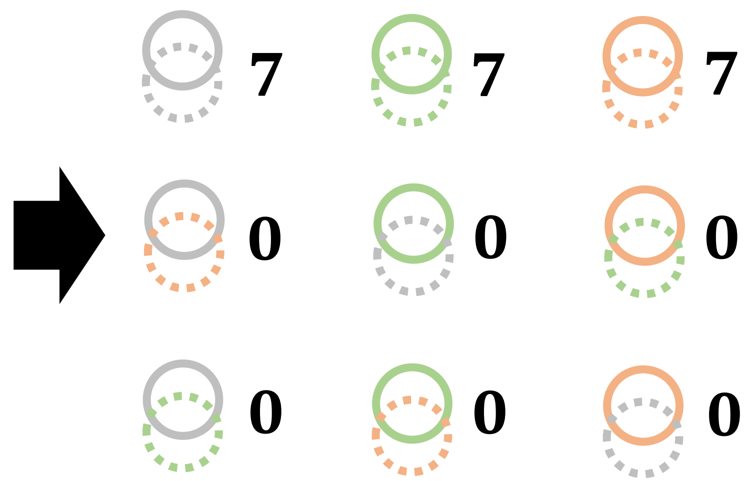
$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$



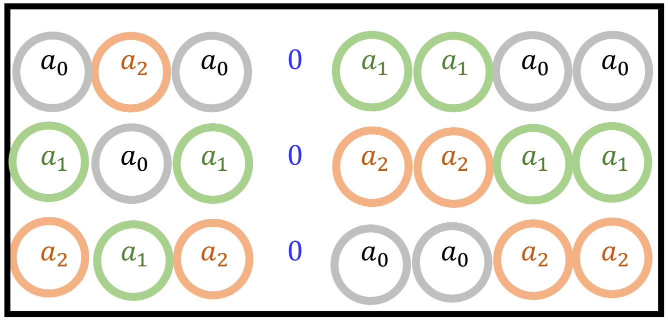
$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$





Autocorrelation of characteristic sequence

s_t

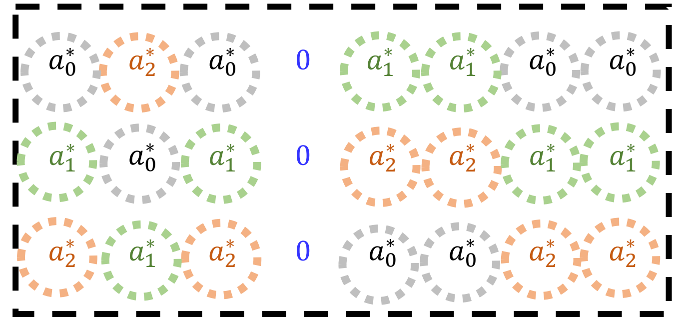


$\boldsymbol{\tau = 0}$

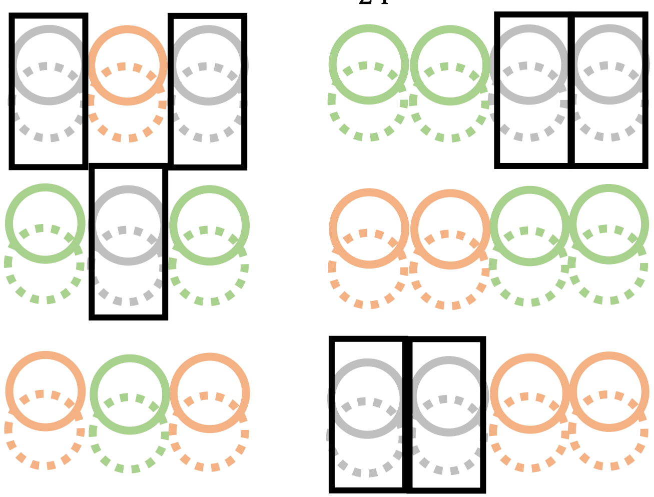
$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

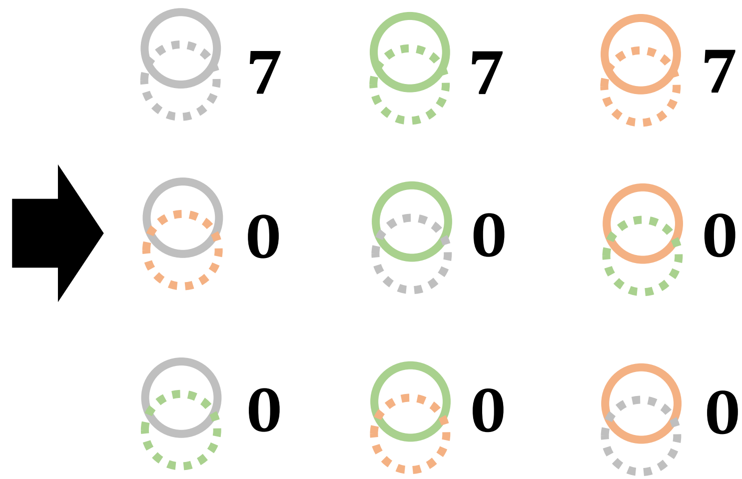
$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$

$s_{t-\tau}^*$



$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s_{t-\tau}^*$$





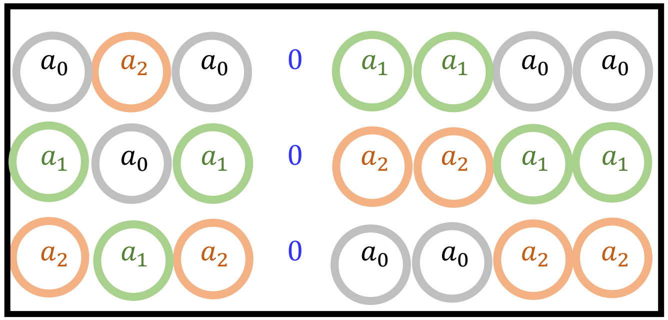
$$C_s(0) = 7(a_0 a_0^* + a_1 a_1^* + a_2 a_2^*) = 7C_a(0)$$

Autocorrelation of characteristic sequence

s_t

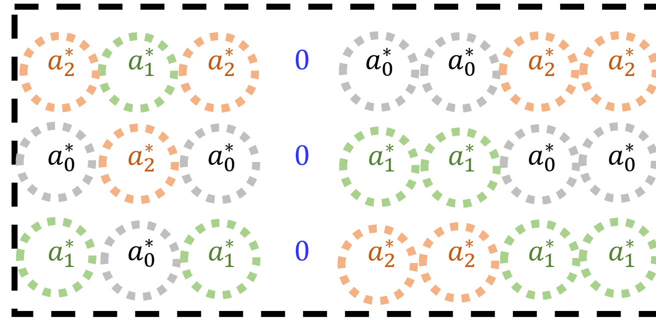
$\boldsymbol{\tau = 8}$

$s^*_{t-\tau}$

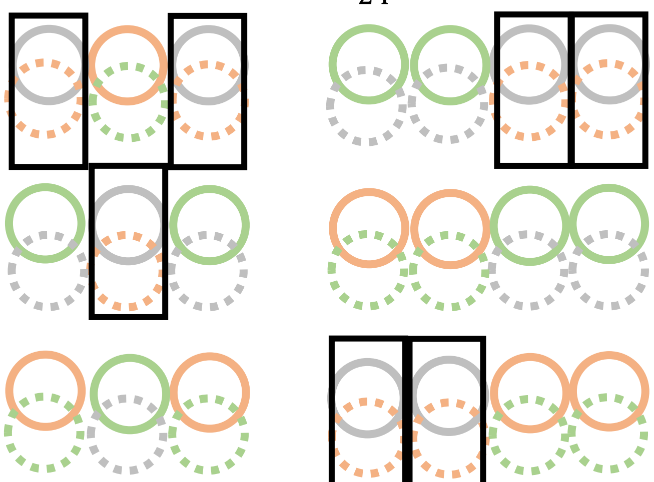


$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$

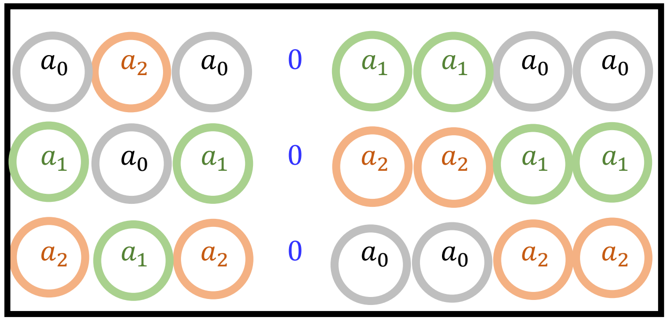


$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$



Autocorrelation of characteristic sequence

s_t

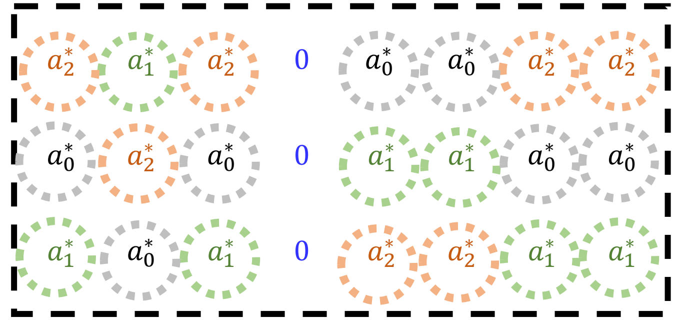


$\boldsymbol{\tau = 8}$

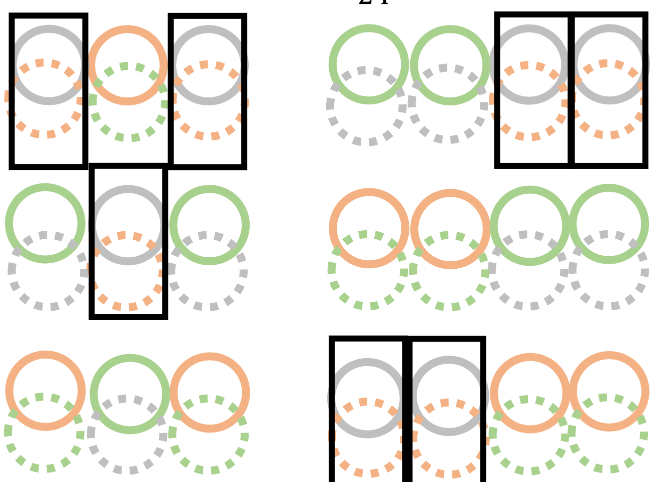
$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

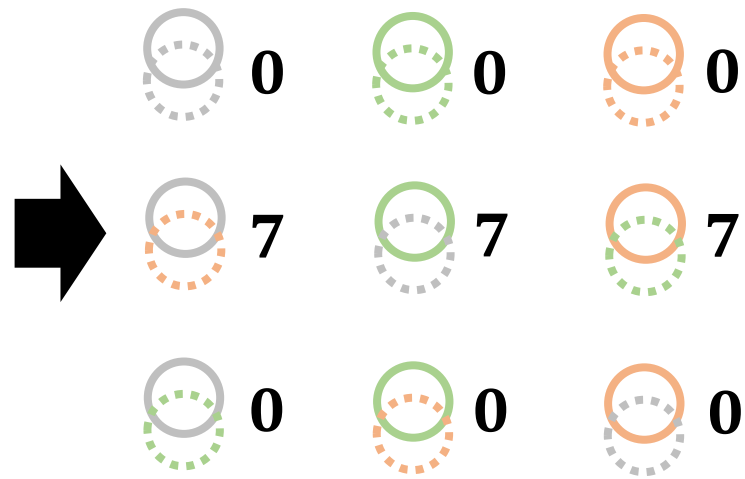
$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$

$s^*_{t-\tau}$



$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$

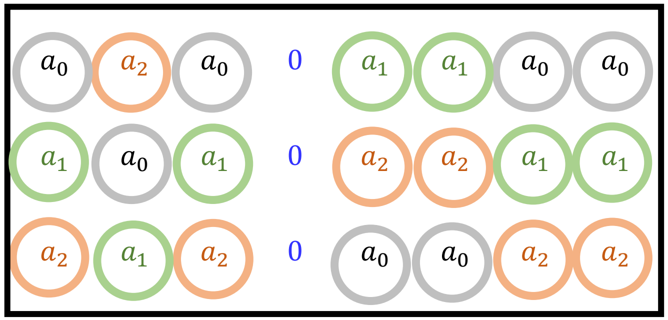




$$C_s(8) = 7(a_0 a_2^* + a_1 a_0^* + a_2 a_1^*) = 7C_a(1)$$

Autocorrelation of characteristic sequence

s_t

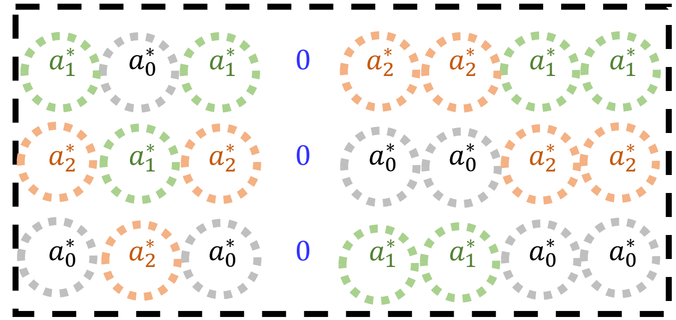


$\boldsymbol{\tau = 16}$

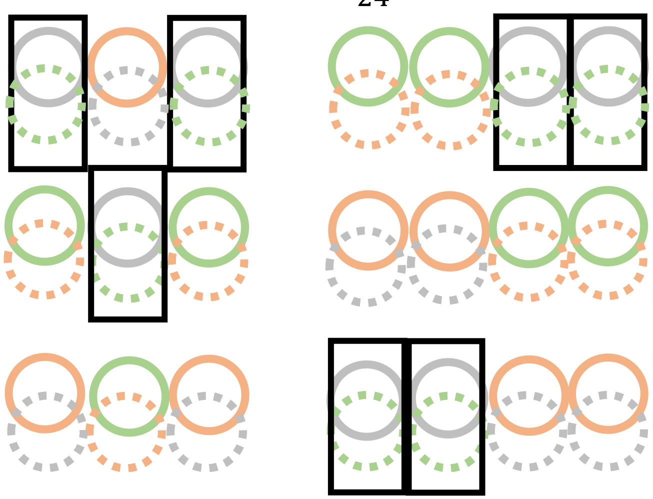
$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

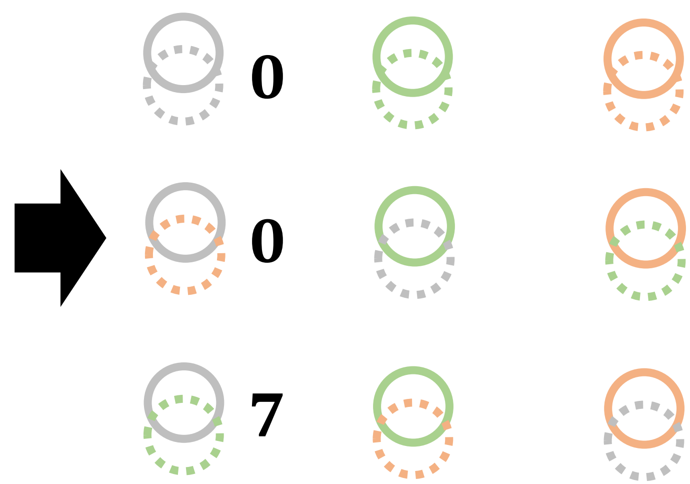
$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$

$s^*_{t-\tau}$



$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$

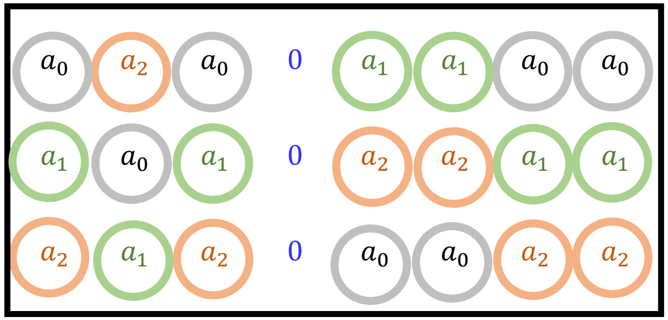




Autocorrelation of characteristic sequence

$\boldsymbol{\tau = 16}$

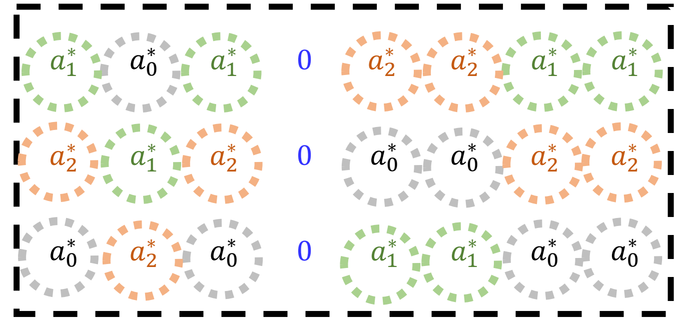
s_t



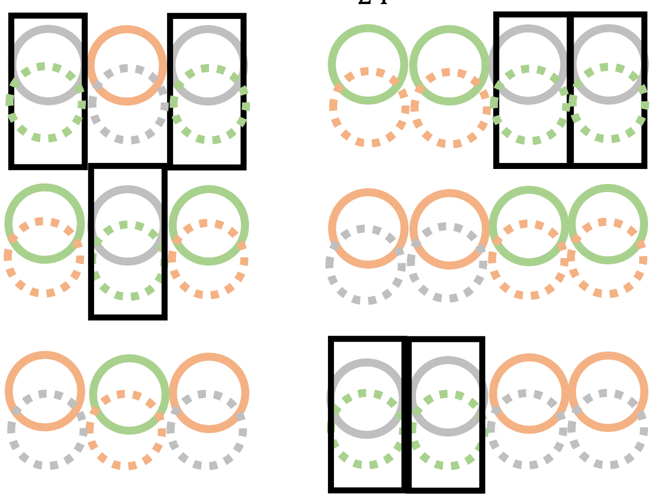
$\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}$

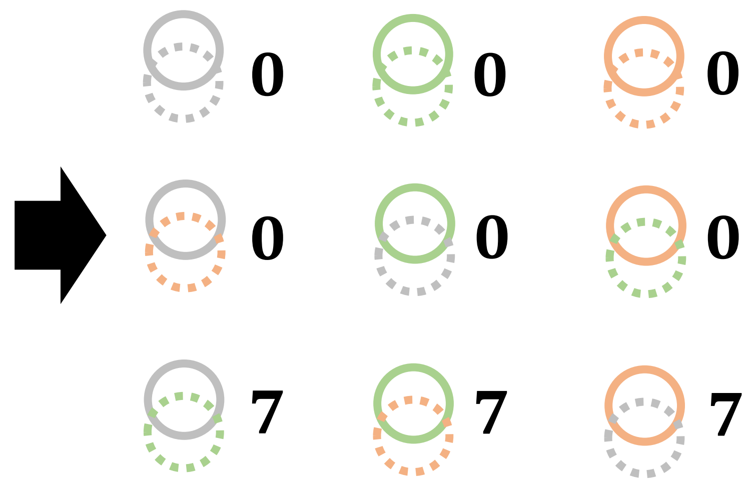
$\boldsymbol{\tau \in 8\mathbb{Z}_{24}}$

$s_{t-\tau}^*$



$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s_{t-\tau}^*$$

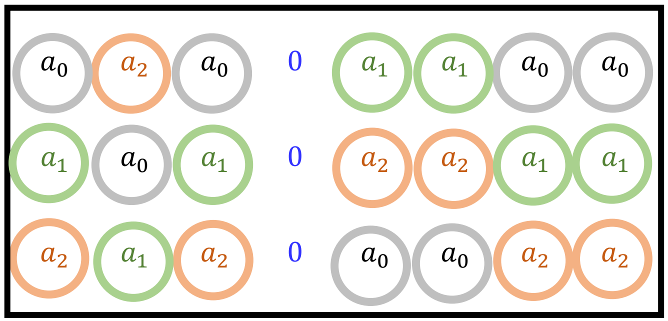




$$C_s(16) = 7(a_0 a_1^* + a_1 a_2^* + a_2 a_0^*) = 7C_a(2)$$

Autocorrelation of characteristic sequence

s_t

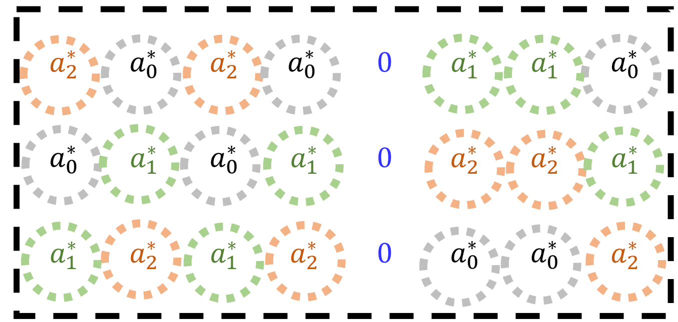


$\boldsymbol{\tau = 1}$

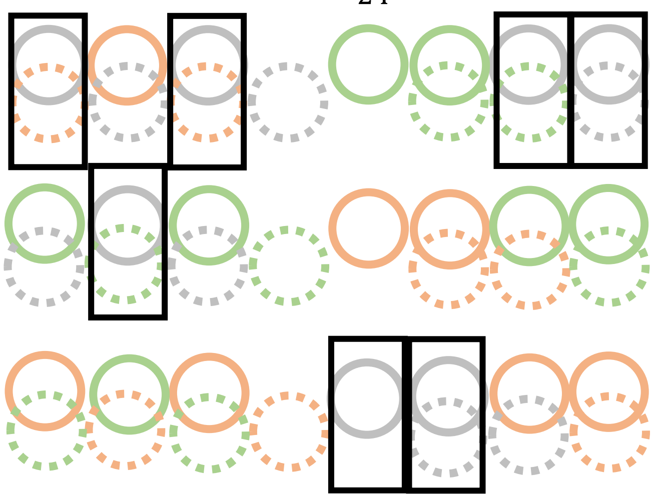
$\boldsymbol{\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}}$

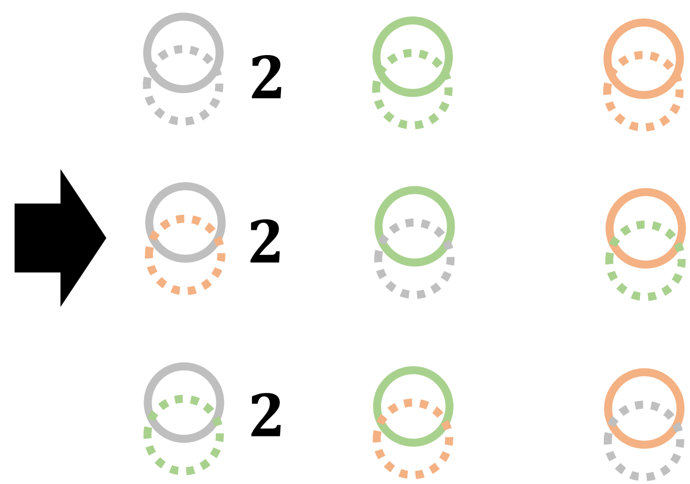
$\tau \in 8\mathbb{Z}_{24}$

$s_{t-\tau}^*$



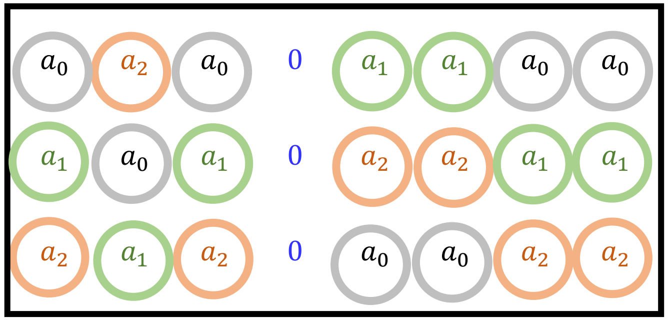
$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s_{t-\tau}^*$$





Autocorrelation of characteristic sequence

s_t

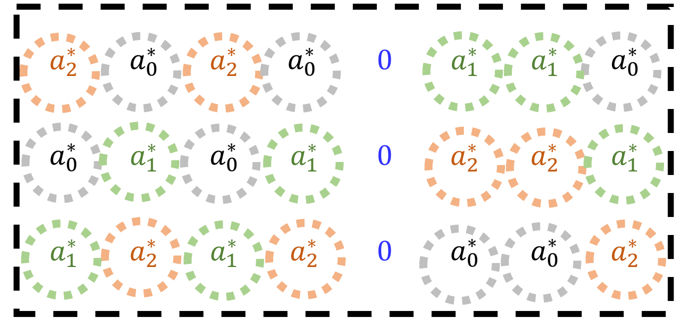


$\boldsymbol{\tau = 1}$

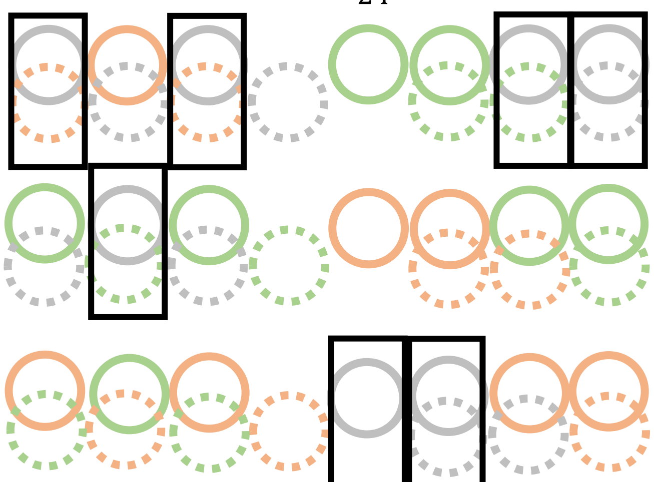
$\boldsymbol{\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}}$

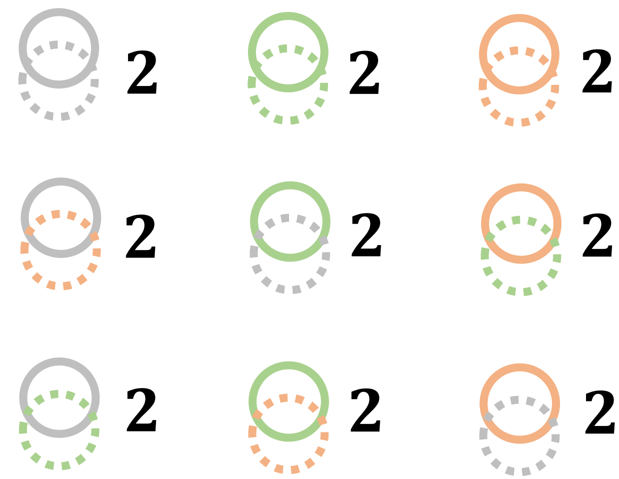
$\tau \in 8\mathbb{Z}_{24}$

$s^*_{t-\tau}$



$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$



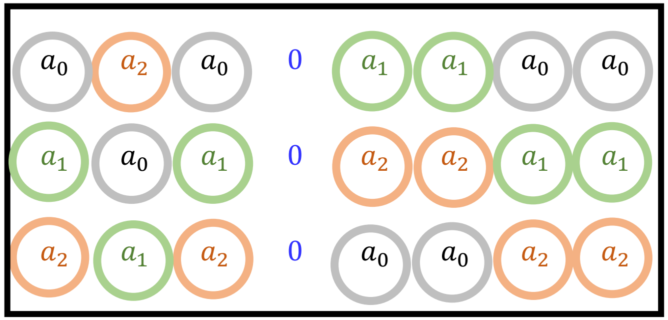


$$C_s(1) = 2\left(\sum_{i \in \mathbb{Z}_3} a_i\right)\left(\sum_{i \in \mathbb{Z}_3} a_i^*\right)$$

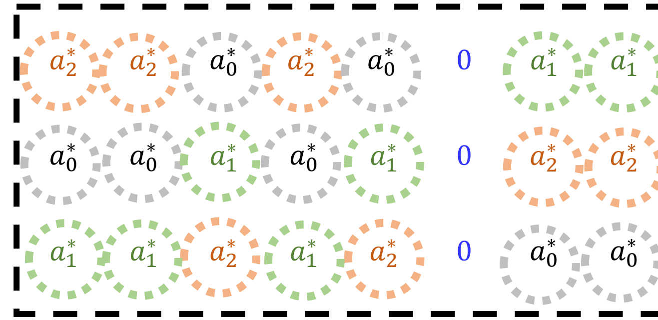
Autocorrelation of characteristic sequence

$\boldsymbol{\tau = 2}$

s_t



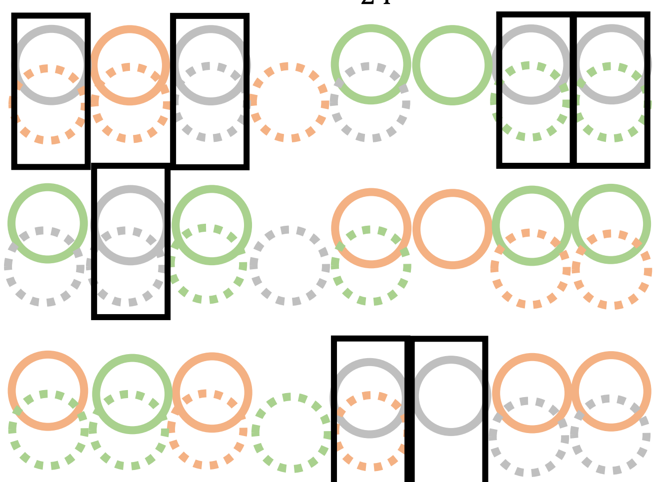
$s^*_{t-\tau}$

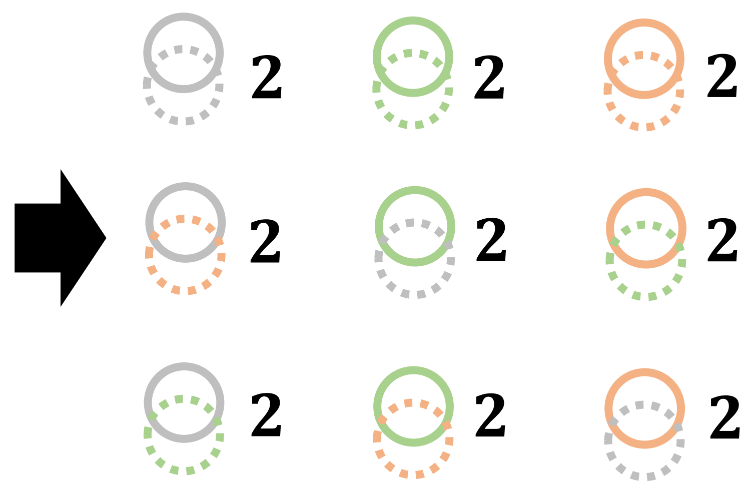


$\boldsymbol{\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}}$

$\tau \in 8\mathbb{Z}_{24}$

$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s^*_{t-\tau}$$



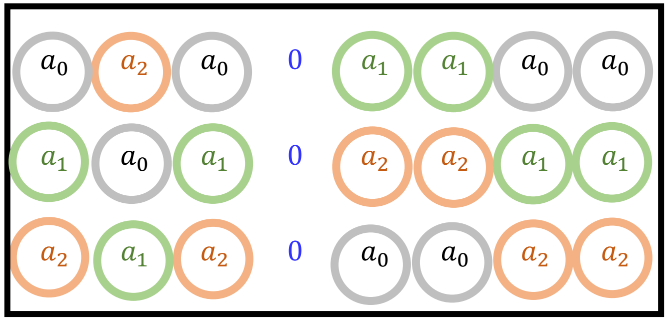


$$C_s(1) = 2\left(\sum_{i \in \mathbb{Z}_3} a_i\right)\left(\sum_{i \in \mathbb{Z}_3} a_i^*\right)$$

Autocorrelation of characteristic sequence

$\boldsymbol{\tau = 3}$

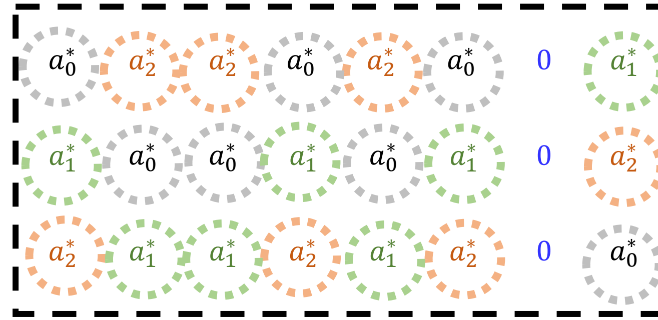
s_t



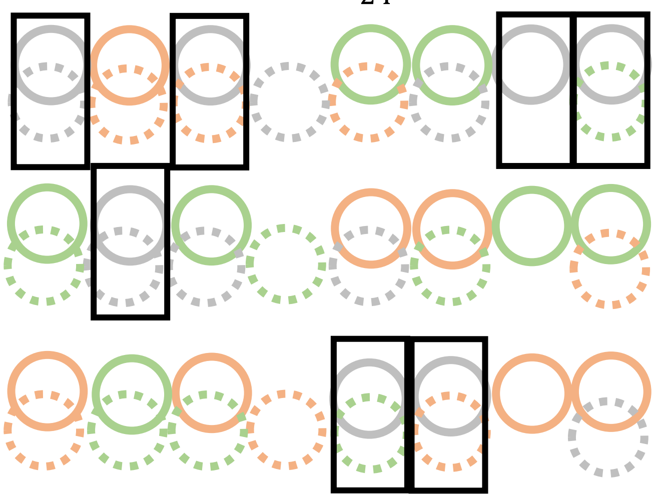
$\boldsymbol{\tau \in \mathbb{Z}_{24} \backslash 8\mathbb{Z}_{24}}$

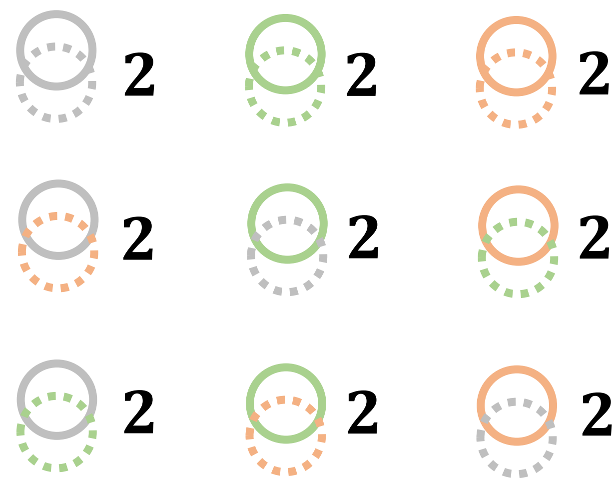
$\tau \in 8\mathbb{Z}_{24}$

$s_{t-\tau}^*$



$$C_s(\tau) = \sum_{t \in \mathbb{Z}_{24}} s_t s_{t-\tau}^*$$





$$C_s(1) = 2\left(\sum_{i \in \mathbb{Z}_3} a_i\right)\left(\sum_{i \in \mathbb{Z}_3} a_i^*\right)$$

Autocorrelation of characteristic sequence

$\boldsymbol{\tau = 3}$

s_t $\quad$ $s^*_{t-\tau}$

Let D be a (u, v, k, λ)-RDS
Let $\boldsymbol{a}$ be a sequence of length v
Let $\boldsymbol{s}$ be a sequence associated with (a, D)

Then,

$$C_{\boldsymbol{s}}(\tau) = \begin{cases} kC_{\boldsymbol{a}}(l), & \text{for some } lu, 0 \le l < v, \\ \lambda\left(\sum_{i\in\mathbb{Z}_v} a_i\right)\left(\sum_{i\in\mathbb{Z}_v} a_i\right)^*, & \text{otherwise,} \end{cases}$$

$$C_{\boldsymbol{s}}(1) = 2\left(\sum_{i\in\mathbb{Z}_3} a_i\right)\left(\sum_{i\in\mathbb{Z}_3} a_i^*\right)$$

Autocorrelation of characteristic sequence

$\boldsymbol{\tau = 3}$

s_t $\qquad$ $s^*_{t-\tau}$

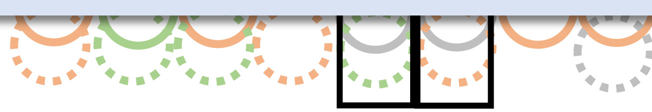
Similarly,

Let $\boldsymbol{s}$ be a sequence associated with $(\boldsymbol{a}, D)$

Let $\boldsymbol{r}$ be a sequence associated with $(\boldsymbol{b}, D)$

Then,

$$C_{\boldsymbol{s},\boldsymbol{r}}(\tau) = \begin{cases} kC_{\boldsymbol{a},\boldsymbol{b}}(l), & \text{for some } lu, 0 \le l < v, \\ \lambda\left(\sum_{i\in\mathbb{Z}_v} a_i\right)\left(\sum_{i\in\mathbb{Z}_v} b_i\right)^*, & \text{otherwise,} \end{cases}$$



$$C_{\boldsymbol{s}}(1) = 2\left(\sum_{i\in\mathbb{Z}_3} a_i\right)\left(\sum_{i\in\mathbb{Z}_3} a_i^*\right)$$

Lemma 1

Lemma 1

Let D be a (u, v, k, λ)-RDS in $\mathbb{Z}_{uv}$ and assume that we are given a family of sequence $\mathcal{A} = \{\mathbf{a}^{(0)}, \mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(T-1)}\}$ all of length v. For each $i = 0, 1, \ldots, T-1$, we define a sequence $\boldsymbol{s}^{(i)}$ as a sequence associated with $(\mathbf{a}^{(i)}, D)$. Then, the correlation of $\boldsymbol{s}^{(i)}$ and $\boldsymbol{s}^{(j)}$ for any $0 \leq i, j < T$ becomes the following:

$$C_{\boldsymbol{s}^{(i)},\boldsymbol{s}^{(j)}}(\tau) = \begin{cases} kC_{\mathbf{a}^{(i)},\mathbf{a}^{(j)}}(l), & \text{for some } lu, 0 \leq l < v, \\ \lambda A_i A_j^*, & \text{otherwise,} \end{cases}$$

where $A_i \triangleq \sum_{h=0}^{v-1} a_h^{(i)}$.

Lemma 1

Lemma 1

Let D be a (u, v, k, λ)-RDS in $\mathbb{Z}_{uv}$ and assume that we are ... $)\}$ all of ... sequence ... hen, the correlation of $\boldsymbol{s}^{(i)}$ and $\boldsymbol{s}^{(j)}$ for any $0 \le i, j < T$ becomes the following:

$$C_{\boldsymbol{s}^{(i)},\boldsymbol{s}^{(j)}}(\tau) = \begin{cases} kC_{\mathbf{a}^{(i)},\mathbf{a}^{(j)}}(l), & \text{for some } lu, 0 \le l < v, \\ \lambda A_i A_j^*, & \text{otherwise,} \end{cases}$$

where $A_i \triangleq \sum_{h=0}^{v-1} a_h^{(i)}$ ...

We hope that $C_{\mathbf{a}^{(i)},\mathbf{a}^{(j)}}(l) = 0$ for $i \ne j$ and all l

We hope that $A_i \triangleq \sum_{h=0}^{v-1} a_h^{(i)} = 0$ for all i

Lemma 1

Let D be a (u, v, k, λ)-RDS in $\mathbb{Z}_{uv}$ and assume that we are ... $)\}$ all of ... sequence ... hen, the correlation of $\boldsymbol{s}^{(i)}$ and $\boldsymbol{s}^{(j)}$ for any $0 \le i, j < T$ becomes the following:

Uncorrelated

We hope that $C_{\mathbf{a}^{(i)},\mathbf{a}^{(j)}}(l) = 0$ for $i \neq j$ and all l

$$C_{\boldsymbol{s}^{(i)},\boldsymbol{s}^{(j)}}(\tau) = \begin{cases} kC_{\mathbf{a}^{(i)},\mathbf{a}^{(j)}}(l), & \text{for some } lu, 0 \le l < v, \\ \lambda A_i A_j^*, & \text{otherwise,} \end{cases}$$

where $A_i \triangleq \sum_{h=0}^{v-1} a_h^{(i)}$ ...

Sum-zero

We hope that $A_i \triangleq \sum_{h=0}^{v-1} a_h^{(i)} = 0$ for all i

Lemma 1

Uncorrelated

We h

We want to find an **uncorrelated** and **sum-zero** sequence family $\mathcal{A} = \{\boldsymbol{a}^{(0)}, \boldsymbol{a}^{(1)}, \ldots\}$

Sum-zero

We hope that $A_i \triangleq \sum_{h=0}^{v-1} a_h^{(i)} = 0$ for all i

Lemma 1

We want to find an **uncorrelated** and **sum-zero** sequence family $\mathcal{A} = \{\boldsymbol{a}^{(0)}, \boldsymbol{a}^{(1)}, \dots\}$

Observe the DFT matrix !

DFT matrix

Proposition (DFT matrix)
1) sum-zero

$$
\begin{array}{c}
\boldsymbol{f}^{(0)} \\ \boldsymbol{f}^{(1)} \\ \boldsymbol{f}^{(2)} \\ \vdots \\ \boldsymbol{f}^{(i)} \\ \vdots \\ \boldsymbol{f}^{(j)} \\ \vdots \\ \boldsymbol{f}^{(v-1)}
\end{array}
\begin{pmatrix}
\omega^0 & \omega^0 & \omega^0 & \cdots & \omega^0 \\
\omega^0 & \omega^1 & \omega^2 & \cdots & \omega^{v-1} \\
\omega^0 & \omega^2 & \omega^4 & \cdots & \omega^{v-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\omega^0 & \omega^i & \omega^{2i} & \cdots & \omega^{(v-1)i} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\omega^0 & \omega^j & \omega^{2j} & \cdots & \omega^{(v-1)j} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\omega^0 & \omega^{v-1} & \omega^{v-2} & \cdots & \omega^1
\end{pmatrix}
$$

$v \times v$ **DFT matrix**

$\sum_{t=0}^{v-1} \omega^0 = v$ — Not sum-zero

$\sum_{t=0}^{v-1} \omega^t = 0$

$\sum_{t=0}^{v-1} \omega^{2t} = 0$

$\vdots$

$\sum_{t=0}^{v-1} \omega^{it} = 0$

$\vdots$

$\sum_{t=0}^{v-1} \omega^{jt} = 0$

$\vdots$

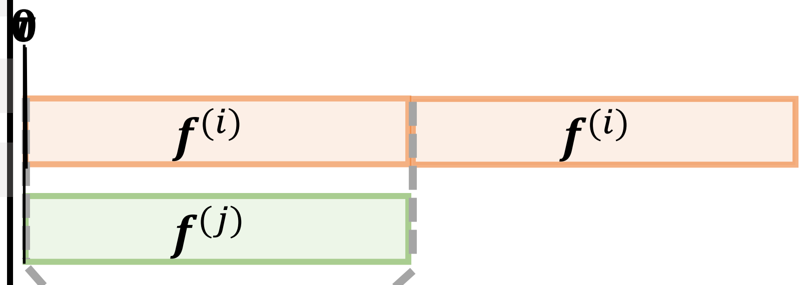
$\sum_{t=0}^{v-1} \omega^{(v-1)t} = 0$

sum-zero

DFT matrix

Proposition (DFT matrix)
2) Uncorrelated property

$$
\begin{array}{c}
f^{(0)} \\ f^{(1)} \\ f^{(2)} \\ \vdots \\ f^{(i)} \\ \vdots \\ f^{(j)} \\ \vdots \\ f^{(v-1)}
\end{array}
\begin{pmatrix}
\omega^0 & \omega^0 & \omega^0 & \cdots & \omega^0 \\
\omega^0 & \omega^1 & \omega^2 & \cdots & \omega^{v-1} \\
\omega^0 & \omega^2 & \omega^4 & \cdots & \omega^{v-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\omega^0 & \omega^i & \omega^{2i} & \cdots & \omega^{(v-1)i} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\omega^0 & \omega^j & \omega^{2j} & \cdots & \omega^{(v-1)j} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\omega^0 & \omega^{v-1} & \omega^{v-2} & \cdots & \omega^1
\end{pmatrix}
$$



$C_{f^{(i)},f^{(j)}}(\tau) = 0$

Cross-correlation value is equal to zero for any shift τ.

$\{f^{(1)}, f^{(2)}, \dots, f^{(v-1)}\}$

is **uncorrelated** sequence family

Main construction

Theorem (Main construction)

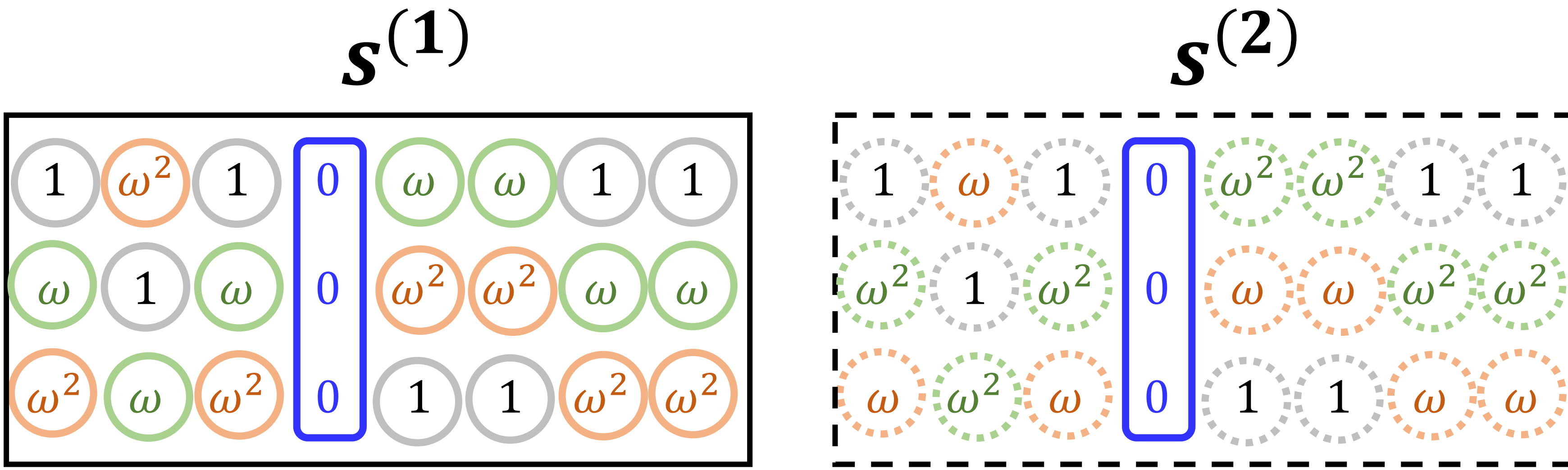
Let D be a (u, v, k, λ) -RDS in $\mathbb{Z}_{uv}$ Let $\mathcal{F} = \{\boldsymbol{f}^{(1)}, \boldsymbol{f}^{(2)}, \dots, \boldsymbol{f}^{(v-1)}\}$ be the set of $v-1$ vectors of length v except for the all-one vector $\boldsymbol{f}^{(0)}$ from the $v \times v$ DFT matrix, let $\boldsymbol{s}^{(\mathrm{i})}$ be the characteristic sequence associated with $(\boldsymbol{f}^{(i)}, D)$. Then $\mathcal{S} = \{\boldsymbol{s}^{(1)}, \boldsymbol{s}^{(2)}, \dots, \boldsymbol{s}^{(v-1)}\}$ is an almost-polyphase uncorrelated $(uv, v-1, u)$-ZCZ sequences family, where the autocorrelation of $\boldsymbol{s}^{(i)}$ for any $1 \le i < v$ becomes following:

$$C_{\boldsymbol{s}^{(\mathrm{i})}}(\tau) = \begin{cases} kv\omega^{il}, & \tau = lu \text{ for some } l \\ 0, & \text{otherwise,} \end{cases}$$

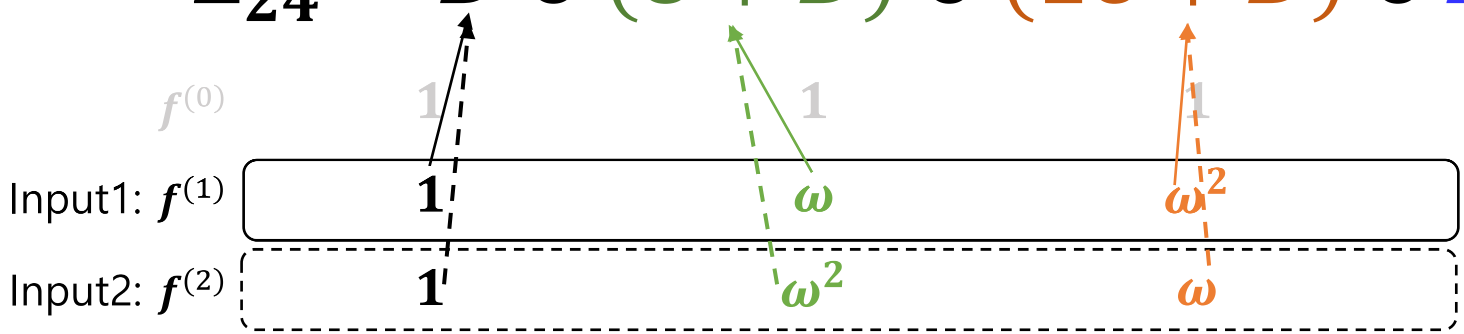
where ω is a complex primitive v-root of unity.

Main construction

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS



$$\mathbb{Z}_{24} = D \cup (8 + D) \cup (16 + D) \cup X$$



3 × 3 DFT matrix

Main construction

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$s^{(1)}$

1	ω^2	1	0	ω	ω	1	1
ω	1	ω	0	ω^2	ω^2	ω	ω
ω^2	ω	ω^2	0	1	1	ω^2	ω^2

$s^{(2)}$

1	ω	1	0	ω^2	ω^2	1	1
ω^2	1	ω^2	0	ω	ω	ω^2	ω^2
ω	ω^2	ω	0	1	1	ω	ω

Cross-correlation

$C_{s^{(1)}, s^{(2)}}(\tau)$

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Uncorrelated

Main construction

$D = \{0, 2, 6, 7, 9, 20, 21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$s^{(1)}$

1	ω^2	1	0	ω	ω	1	1
ω	1	ω	0	ω^2	ω^2	ω	ω
ω^2	ω	ω^2	0	1	1	ω^2	ω^2

$s^{(2)}$

1	ω	1	0	ω^2	ω^2	1	1
ω^2	1	ω^2	0	ω	ω	ω^2	ω^2
ω	ω^2	ω	0	1	1	ω	ω

Autocorrelation

Autocorrelation

Zone Size: u = 8

$C_{s^{(1)}}(\tau)$

21	0	0	0	0	0	0	0
21ω	0	0	0	0	0	0	0
$21\omega^2$	0	0	0	0	0	0	0

$C_{s^{(2)}}(\tau)$

21	0	0	0	0	0	0	0
$21\omega^2$	0	0	0	0	0	0	0
21ω	0	0	0	0	0	0	0

Main construction

$D = \{0,2,6,7,9,20,21\}$: $(u = 8, v = 3, k = 7, \lambda = 2)$-RDS

$s^{(1)}$

1	ω^2	1	0	ω	ω	1	1
ω	1	ω	0	ω^2	ω^2	ω	ω
ω^2	ω	ω^2	0	1	1	ω^2	ω^2

$s^{(2)}$

1	ω	1	0	ω^2	ω^2	1	1
ω^2	1	ω^2	0	ω	ω	ω^2	ω^2
ω	ω^2	ω	0	1	1	ω	ω

Autocorrelation

Autocorrelation

$C_{s^{(1)}}(\tau)$

Zone Size: u = 8

$C_{s^{(2)}}(\tau)$

21 0 0 … 0 0

21ω 0 0 … 0 0

$21\omega^2$ 0 0 … 0 0

Therefore, $\{s^{(0)}, s^{(1)}\}$ is an uncorrelated (24,2,8)-ZCZ sequences family.

Specification of our construction.

Specification of our construction.

Let q be a prime power, v be a divisor of $q-1$ or $2(q-1)$ for any prime power q or (even $q=p^n$ and odd n), respectively. Then **Theorem 1** construct some uncorrelated ZCZ sequences family with the following parameters:

1) $L=\frac{q^n-1}{q-1}v, K=v-1, W=\frac{q^n-1}{q-1}$.

2) Alphabet size is $v+1$. That is, every symbol in the sequences is expressed as 0 or ω_v^k for $k=0,1,\ldots,v-1$.

3) The number of 0's in each sequence is $L\frac{q^{n-1}-1}{q^n-1}$.

This sequence is almost-optimal because

$$K=\frac{L}{W}-1.\ \ \text{(Note that } K\leq\frac{L}{W}\text{)}$$

Comparison with other well known uncorrelated ZCZ sequences family

Construction	Construction	Length(L)	Family size(K)	Zone size(W)	Alphabet size
Optimal Polyphase	Suehiro [44]	KZ	K	Z	KZ or $2KZ$ $(>\sqrt{KL})$
	Brodzik [5]	p^3	p	p^2	$p^2(=\sqrt{KL})$
	Brodzik [6]	KZ	K	Z	KZ or $2KZ$ $(>\sqrt{KL})$
	Popovic [33]	KZ	K	Z	KZ or $2KZ$ $(>\sqrt{KL})$
	Zhang [53]$^{(c)}$	KZ	K	Z	KZ or $2KZ$ $(>\sqrt{KL})$
	Fang and Wang [12]	KZ^2	K	Z^2	KZ $(=\sqrt{KL})$
Almost-Otimal and Almost-Polyphase	Tirkel et al. [47]	q^n-1	$q-2$	$\frac{q^n-1}{q-1}$	q $(<\sqrt{KL})$
	Construction 1 (Theorem 1)	$\frac{q^n-1}{q-1}v$	$v-1$	$\frac{q^n-1}{q-1}$	v+1 $(<\sqrt{KL})$