Card Shuffle Groups

Wenying Zhu

Beijing Normal University

This is joint work with Binzhou Xia and Zhishuo Zhang.

7 Nov 2023, Seminar (Online)

Perfectly shuffle $2n$ cards

- Cut the deck in half:

$$\begin{array}{r} 0\,\text{—} \\ 1\,\text{—} \\ \vdots \\ 2n-1\,\text{—} \end{array} \quad \longrightarrow \quad \begin{array}{rl} 0\,\text{—} & \text{—}\,n \\ 1\,\text{—} & \text{—}\,n+1 \\ \vdots & \vdots \\ n-1\,\text{—} & \text{—}\,2n-1 \end{array}$$

- Perfectly interleave them:

$$\begin{array}{rl} 0\,\text{—} & \\ & \text{—}\,n \\ 1\,\text{—} & \\ & \text{—}\,n+1 \\ \vdots & \\ n-1\,\text{—} & \\ & \text{—}\,2n-1 \end{array} \qquad\qquad \begin{array}{rl} & \text{—}\,n \\ 0\,\text{—} & \\ & \text{—}\,n+1 \\ 1\,\text{—} & \\ \vdots & \\ & \text{—}\,2n-1 \\ n-1\,\text{—} & \end{array}$$

Out-shuffle O In-shuffle I

Questions

Perform out-shuffles on a deck of 52 cards repeatedly.

Questions

Perform out-shuffles on a deck of 52 cards repeatedly.

Question: Can it return to the original order?

Questions

Perform out-shuffles on a deck of 52 cards repeatedly.

Question: Can it return to the original order?

Answer: Yes. For example, after 52! times.

Questions

Perform out-shuffles on a deck of 52 cards repeatedly.

Question: Can it return to the original order?

Answer: Yes. For example, after 52! times.

Question: What is the minimum number of times needed to return to the original order?

Questions

Perform out-shuffles on a deck of 52 cards repeatedly.

Question: Can it return to the original order?

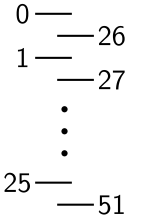
Answer: Yes. For example, after 52! times.

Question: What is the minimum number of times needed to return to the original order?

Answer: 8 times.

Why 8 times

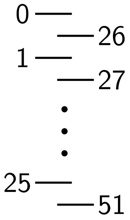
- Position x: 0 1 2 3 4 $\cdots$ 25 26 $\cdots$ 50 51



Out-shuffle O

Why 8 times

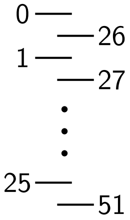
- Position x: 0 $\quad$ 1 $\quad$ 2 $\quad$ 3 $\quad$ 4 $\cdots$ 25 $\quad$ 26 $\cdots$ 50 $\quad$ 51



Out-shuffle O

Why 8 times

Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51

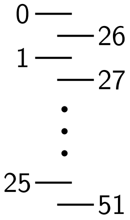


Out-shuffle O

Why 8 times

- Position x:

Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51
x^O:	0	2	4	6	8	$\cdots$	50	1	$\cdots$	49	51



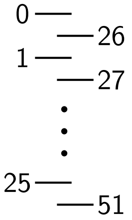
Out-shuffle O

Why 8 times

- Position x: / after O: / x^O:

Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51
x^O:	0	2	4	6	8	$\cdots$	50	1	$\cdots$	49	51

- $(i + 26j)^O = 2i + j$ for $i \in \{0, \ldots, 25\}$ and $j \in \{0, 1\}$;

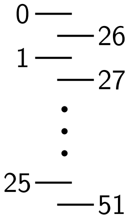


Out-shuffle O

Why 8 times

Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51
x^O:	0	2	4	6	8	$\cdots$	50	1	$\cdots$	49	51

- $(i + 26j)^O = 2i + j$ for $i \in \{0, \ldots, 25\}$ and $j \in \{0, 1\}$;
- $0^O = 0$ and $51^O = 51$;



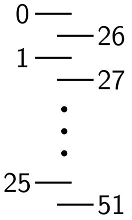
Out-shuffle O

Why 8 times

-

Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51
x^O:	0	2	4	6	8	$\cdots$	50	1	$\cdots$	49	51

- $(i + 26j)^O = 2i + j$ for $i \in \{0, \dots, 25\}$ and $j \in \{0, 1\}$;
- $0^O = 0$ and $51^O = 51$;
- $x^O = (2x \bmod 51)$ for $x \in \{1, \dots, 50\}$;



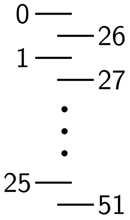
Out-shuffle O

Why 8 times

- Position x, after O, and x^O:

Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51
x^O:	0	2	4	6	8	$\cdots$	50	1	$\cdots$	49	51

- $(i + 26j)^O = 2i + j$ for $i \in \{0, \ldots, 25\}$ and $j \in \{0, 1\}$;
- $0^O = 0$ and $51^O = 51$;
- $x^O = (2x \bmod 51)$ for $x \in \{1, \ldots, 50\}$;
- the order of O is the smallest positive integer t such that $2^t \equiv 1 \pmod{51}$.

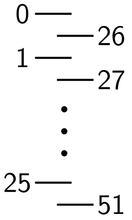


Out-shuffle O

Why 8 times

• Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51
x^O:	0	2	4	6	8	$\cdots$	50	1	$\cdots$	49	51

- $(i + 26j)^O = 2i + j$ for $i \in \{0, \ldots, 25\}$ and $j \in \{0, 1\}$;
- $0^O = 0$ and $51^O = 51$;
- $x^O = (2x \bmod 51)$ for $x \in \{1, \ldots, 50\}$;
- the order of O is the smallest positive integer t such that $2^t \equiv 1 \pmod{51}$.



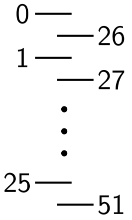
Out-shuffle O

- $(i + jn)^O = 2i + j$ for $i \in \{0, \ldots, n-1\}$ and $j \in \{0, 1\}$;

Why 8 times

Position x:	0	1	2	3	4	$\cdots$	25	26	$\cdots$	50	51
after O:	0	26	1	27	2	$\cdots$	38	13	$\cdots$	25	51
x^O:	0	2	4	6	8	$\cdots$	50	1	$\cdots$	49	51

- $(i + 26j)^O = 2i + j$ for $i \in \{0, \ldots, 25\}$ and $j \in \{0, 1\}$;
- $0^O = 0$ and $51^O = 51$;
- $x^O = (2x \bmod 51)$ for $x \in \{1, \ldots, 50\}$;
- the order of O is the smallest positive integer t such that $2^t \equiv 1 \pmod{51}$.



Out-shuffle O

- $(i + jn)^O = 2i + j$ for $i \in \{0, \ldots, n-1\}$ and $j \in \{0, 1\}$;
- $x^O = (2\ell \bmod 2n - 1)$ for $x \in \{1, \ldots, 2n-2\}$.

More questions

Question: Is it possible to send a given card to any chosen position by performing a sequence of the two shuffles?

More questions

Question: Is it possible to send a given card to any chosen position by performing a sequence of the two shuffles?

Answer: Yes.

More questions

Question: Is it possible to send a given card to any chosen position by performing a sequence of the two shuffles?

Answer: Yes.

Question: Can we obtain all different orderings by performing a sequence of the two shuffles?

More questions

Question: Is it possible to send a given card to any chosen position by performing a sequence of the two shuffles?

Answer: Yes.

Question: Can we obtain all different orderings by performing a sequence of the two shuffles?

If it is not possible, then

More questions

Question: Is it possible to send a given card to any chosen position by performing a sequence of the two shuffles?

Answer: Yes.

Question: Can we obtain all different orderings by performing a sequence of the two shuffles?

If it is not possible, then

Question: How many/Which orderings can be obtained by performing a sequence of the two shuffles?

More questions

Question: Is it possible to send a given card to any chosen position by performing a sequence of the two shuffles?

Answer: Yes.

Question: Can we obtain all different orderings by performing a sequence of the two shuffles?

If it is not possible, then

Question: How many/Which orderings can be obtained by performing a sequence of the two shuffles?

To answer these questions, we first determine the parity of O and I.

Observation

Observation: for $n = 4$,

Position x:	0	1	2	3	4	5	6	7
after O:	0	4	1	5	2	6	3	7
x^O:	0	2	4	6	1	3	5	7

Observation

Observation: for $n = 4$,

- Position x: 0 1 2 3 4 5 6 7

Position x:	0	1	2	3	4	5	6	7
after O:	0	4	1	5	2	6	3	7
x^O:	0	2	4	6	1	3	5	7

- the inversion number of (0,2,4,6,1,3,5,7) is $1 + 2 + 3$.

Observation

Observation: for $n = 4$,

- Position x: 0 1 2 3 4 5 6 7
  after O: 0 4 1 5 2 6 3 7
  x^O: 0 2 4 6 1 3 5 7
- the inversion number of (0,2,4,6,1,3,5,7) is $1 + 2 + 3$.

For general n, the order of the $2n$ cards after O is

$$(0, 2, 4, 6, \ldots, 2n - 2, 1, 3, 5, \ldots, 2n - 1),$$

Observation

Observation: for $n = 4$,

Position x:	0	1	2	3	4	5	6	7
after O:	0	4	1	5	2	6	3	7
x^O:	0	2	4	6	1	3	5	7

- the inversion number of (0,2,4,6,1,3,5,7) is $1 + 2 + 3$.

For general n, the order of the $2n$ cards after O is

$$(0, 2, 4, 6, \ldots, 2n - 2, 1, 3, 5, \ldots, 2n - 1),$$

and thus its inversion number is $1 + \cdots + n - 1 = n(n - 1)/2$.

Parity of O and I

- Inversion number $n(n-1)/2$

Parity of O and I

- Inversion number $n(n-1)/2 \Longrightarrow$ If $n \equiv 0$ or $1 \pmod 4$, then O is even; otherwise O is odd.

Parity of O and I

- Inversion number $n(n-1)/2 \Longrightarrow$ If $n \equiv 0$ or $1 \pmod 4$, then O is even; otherwise O is odd.
- I is obtained by permutating the two piles and then performing O.
  ($x^I = x^{(0,n)(1,n+1)\cdots(n-1,2n-1)O}$ for all $x \in \{0, 1, \ldots, 2n-1\}$)

Parity of O and I

- Inversion number $n(n-1)/2 \Longrightarrow$ If $n \equiv 0$ or $1 \pmod 4$, then O is even; otherwise O is odd.
- I is obtained by permutating the two piles and then performing O. ($x^I = x^{(0,n)(1,n+1)\cdots(n-1,2n-1)O}$ for all $x \in \{0, 1, \ldots, 2n-1\}$)
- The permutation of the $2n$ cards induced by permutating the two piles has the same parity as n.

Parity of O and I

- Inversion number $n(n-1)/2 \Longrightarrow$ If $n \equiv 0$ or $1 \pmod 4$, then O is even; otherwise O is odd.
- I is obtained by permutating the two piles and then performing O. $(x^I = x^{(0,n)(1,n+1)\cdots(n-1,2n-1)O}$ for all $x \in \{0, 1, \ldots, 2n-1\})$
- The permutation of the $2n$ cards induced by permutating the two piles has the same parity as n.
- If n and O have the same parity, then I is even; otherwise I is odd

Parity of O and I

- Inversion number $n(n-1)/2 \Longrightarrow$ If $n \equiv 0$ or $1 \pmod 4$, then O is even; otherwise O is odd.
- I is obtained by permutating the two piles and then performing O. ($x^I = x^{(0,n)(1,n+1)\cdots(n-1,2n-1)O}$ for all $x \in \{0, 1, \ldots, 2n-1\}$)
- The permutation of the $2n$ cards induced by permutating the two piles has the same parity as n.
- If n and O have the same parity, then I is even; otherwise I is odd $\Longrightarrow$ If $n \equiv 0$ or $3 \pmod 4$, then I is even; otherwise I is odd.

Parity of O and I

- Inversion number $n(n-1)/2 \Longrightarrow$ If $n \equiv 0$ or $1 \pmod 4$, then O is even; otherwise O is odd.

- I is obtained by permutating the two piles and then performing O. ($x^I = x^{(0,n)(1,n+1)\cdots(n-1,2n-1)O}$ for all $x \in \{0, 1, \ldots, 2n-1\}$)

- The permutation of the $2n$ cards induced by permutating the two piles has the same parity as n.

- If n and O have the same parity, then I is even; otherwise I is odd $\Longrightarrow$ If $n \equiv 0$ or $3 \pmod 4$, then I is even; otherwise I is odd.

- Thus $\langle O, I \rangle \leq \mathrm{Alt}(2n) \Longleftrightarrow n \equiv 0 \pmod 4$.

Questions on $\langle O, I \rangle$

Question: Can $\langle O, I \rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Questions on $\langle O, I \rangle$

Question: Can $\langle O, I \rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Question: Can $\langle O, I \rangle$ equal $\mathrm{Sym}(2n)$ when $n \not\equiv 0 \pmod 4$?

Questions on $\langle O, I \rangle$

Question: Can $\langle O, I \rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Question: Can $\langle O, I \rangle$ equal $\mathrm{Sym}(2n)$ when $n \not\equiv 0 \pmod 4$?

Answer: Both no.

Questions on $\langle O, I \rangle$

Question: Can $\langle O, I \rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Question: Can $\langle O, I \rangle$ equal $\mathrm{Sym}(2n)$ when $n \not\equiv 0 \pmod 4$?

Answer: Both no.

Observation: for $n = 4$,

- original order: (0,1,2,3,4,5,6,7),

Questions on $\langle O, I\rangle$

Question: Can $\langle O, I\rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Question: Can $\langle O, I\rangle$ equal $\mathrm{Sym}(2n)$ when $n \not\equiv 0 \pmod 4$?

Answer: Both no.

Observation: for $n = 4$,

- original order: (0,1,2,3,4,5,6,7),

  after the out-shuffle: (0,2,4,6,1,3,5,7),

Questions on $\langle O, I \rangle$

Question: Can $\langle O, I \rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Question: Can $\langle O, I \rangle$ equal $\mathrm{Sym}(2n)$ when $n \not\equiv 0 \pmod 4$?

Answer: Both no.

Observation: for $n = 4$,

- original order: (0,1,2,3,4,5,6,7),

  after the out-shuffle: (0,2,4,6,1,3,5,7),

  after the in-shuffle: (1,3,5,7,0,2,4,6);

Questions on $\langle O, I \rangle$

Question: Can $\langle O, I \rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Question: Can $\langle O, I \rangle$ equal $\mathrm{Sym}(2n)$ when $n \not\equiv 0 \pmod 4$?

Answer: Both no.

Observation: for $n = 4$,

- original order: (0,1,2,3,4,5,6,7),

  after the out-shuffle: (0,2,4,6,1,3,5,7),

  after the in-shuffle: (1,3,5,7,0,2,4,6);

- out-shuffle and in-shuffle preserve the partition $\{0, 7\}, \{1, 6\}, \{2, 5\}, \{3, 4\}$.

Questions on $\langle O, I\rangle$

Question: Can $\langle O, I\rangle$ equal $\mathrm{Alt}(2n)$ when $n \equiv 0 \pmod 4$?

Question: Can $\langle O, I\rangle$ equal $\mathrm{Sym}(2n)$ when $n \not\equiv 0 \pmod 4$?

Answer: Both no.

Observation: for $n = 4$,

- original order: (0,1,2,3,4,5,6,7),

  after the out-shuffle: (0,2,4,6,1,3,5,7),

  after the in-shuffle: (1,3,5,7,0,2,4,6);
- out-shuffle and in-shuffle preserve the partition $\{0,7\},\{1,6\},\{2,5\},\{3,4\}$.

For a general n, out-shuffle and in-shuffle preserve the partition $\{0, 2n-1\}, \{1, 2n-2\}, \ldots, \{n-1, n\}$.

$\langle O, I \rangle$ is neither $\mathrm{Alt}(2n)$ nor $\mathrm{Sym}(2n)$

- A permutation group on a set Ω is said to be imprimitive if this group preserves a nontrivial partition of Ω; otherwise, it is said to be primitive.

$\langle O, I \rangle$ is neither $\mathrm{Alt}(2n)$ nor $\mathrm{Sym}(2n)$

- A permutation group on a set Ω is said to be imprimitive if this group preserves a nontrivial partition of Ω; otherwise, it is said to be primitive.

- O and I preserve $\{0, 2n-1\}, \{1, 2n-2\}, \ldots, \{n-1, n\}$

$\langle O, I \rangle$ is neither $\mathrm{Alt}(2n)$ nor $\mathrm{Sym}(2n)$

- A permutation group on a set Ω is said to be imprimitive if this group preserves a nontrivial partition of Ω; otherwise, it is said to be primitive.
- O and I preserve $\{0, 2n-1\}, \{1, 2n-2\}, \ldots, \{n-1, n\}$ $\Longrightarrow \langle O, I \rangle$ is imprimitive.

$\langle O, I \rangle$ is neither $\mathrm{Alt}(2n)$ nor $\mathrm{Sym}(2n)$

- A permutation group on a set Ω is said to be imprimitive if this group preserves a nontrivial partition of Ω; otherwise, it is said to be primitive.

- O and I preserve $\{0, 2n-1\}, \{1, 2n-2\}, \ldots, \{n-1, n\}$ $\Longrightarrow \langle O, I \rangle$ is imprimitive.

- $\mathrm{Alt}(2n)$ is primitive

$\langle O, I\rangle$ is neither $\mathrm{Alt}(2n)$ nor $\mathrm{Sym}(2n)$

- A permutation group on a set Ω is said to be imprimitive if this group preserves a nontrivial partition of Ω; otherwise, it is said to be primitive.
- O and I preserve $\{0, 2n-1\}, \{1, 2n-2\}, \ldots, \{n-1, n\}$ $\Longrightarrow \langle O, I\rangle$ is imprimitive.
- $\mathrm{Alt}(2n)$ is primitive $\Longrightarrow \mathrm{Alt}(2n) \nleq \langle O, I\rangle$

$\langle O, I \rangle$ is neither $\mathrm{Alt}(2n)$ nor $\mathrm{Sym}(2n)$

- A permutation group on a set Ω is said to be imprimitive if this group preserves a nontrivial partition of Ω; otherwise, it is said to be primitive.
- O and I preserve $\{0, 2n-1\}, \{1, 2n-2\}, \ldots, \{n-1, n\}$ $\Longrightarrow \langle O, I \rangle$ is imprimitive.
- $\mathrm{Alt}(2n)$ is primitive $\Longrightarrow \mathrm{Alt}(2n) \nleqslant \langle O, I \rangle \Longrightarrow$ O and I can't generate $\mathrm{Alt}(2n)$ or $\mathrm{Sym}(2n)$.

Diaconis-Graham-Kantor

Question: How many/Which orderings can be obtained by performing a sequence of the two shuffles?

[1] P. Diaconis, R. L. Graham and W. M. Kantor, The mathematics of perfect shuffles., *Adv. Appl. Math.*, 4 (1983), 175–196.

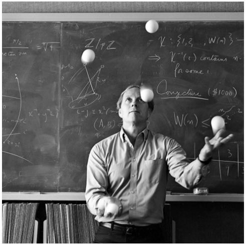
Diaconis-Graham-Kantor

Question: How many/Which orderings can be obtained by performing a sequence of the two shuffles?

Answered by Diaconis, Graham and Kantor in 1983[1].

Persi Diaconis

ICM talk in 1990



Ron Graham

ICM talk in 1983

William M. Kantor

ICM talk in 1998

[1] P. Diaconis, R. L. Graham and W. M. Kantor, The mathematics of perfect shuffles., *Adv. Appl. Math.*, 4 (1983), 175–196.

The classification of $\langle O, I\rangle$ in [1]

Size of each pile n	$\langle O, I\rangle$
$n = 2^f$ for some positive integer f	$C_2 \wr C_{f+1}$
$n \equiv 0 \pmod 4$, $n > 12$ and n is not a power of 2	$C_2^{n-1} \rtimes A_n$
$n \equiv 1 \pmod 4$	$C_2^n \rtimes A_n$
$n \equiv 2 \pmod 4$ and $n > 6$	$C_2 \wr \mathrm{Sym}(n)$
$n \equiv 3 \pmod 4$	$C_2^{n-1} \rtimes S_n$
$n = 6$	$C_2^6 \rtimes \mathrm{PGL}(2,5)$
$n = 12$	$C_2^{11} \rtimes M_{12}$

[1] P. Diaconis, R. L. Graham and W. M. Kantor, The mathematics of perfect shuffles., *Adv. Appl. Math.*, 4 (1983), 175–196.

A deck of kn cards with $k \geq 2$

- cut into k piles and then perfectly interleave them ($k!$ ways).

$$\begin{matrix} 0 \\ 1 \\ \vdots \\ kn-1 \end{matrix} \quad \longrightarrow \quad \begin{matrix} 0 & n & \cdots & (k-1)n \\ 1 & 1+n & \cdots & 1+(k-1)n \\ \vdots & \vdots & & \vdots \\ n-1 & 2n-1 & \cdots & kn-1 \end{matrix}$$

A deck of kn cards with $k \geq 2$

- cut into k piles and then perfectly interleave them ($k!$ ways).

$$\begin{array}{c} 0 \\ 1 \\ \vdots \\ kn-1 \end{array} \quad \longrightarrow \quad \begin{array}{cccc} 0 & n & \cdots & (k-1)n \\ 1 & 1+n & \cdots & 1+(k-1)n \\ \vdots & \vdots & & \vdots \\ n-1 & 2n-1 & \cdots & kn-1 \end{array}$$

- Standard shuffle σ: picking up the top card from each of the piles $0, \ldots, k-1$ in order and repeating until all cards have been picked up.

A deck of kn cards with $k \geq 2$

- cut into k piles and then perfectly interleave them ($k!$ ways).

$$
\begin{array}{c}
0 \\
1 \\
\vdots \\
kn-1
\end{array}
\quad \longrightarrow \quad
\begin{array}{ccccc}
0 & n & \cdots & (k-1)n \\
1 & 1+n & \cdots & 1+(k-1)n \\
\vdots & \vdots & & \vdots \\
n-1 & 2n-1 & \cdots & kn-1
\end{array}
$$

- Standard shuffle σ: picking up the top card from each of the piles $0, \ldots, k-1$ in order and repeating until all cards have been picked up.
- ρ_τ: the permutation of the kn cards induced by the permutation τ of the k piles.

Shuffle groups

- For a positive integer m, denote $[m] = \{0, 1, \ldots, m-1\}$.

Shuffle groups

- For a positive integer m, denote $[m] = \{0, 1, \dots, m-1\}$.
- k piles:

$$\begin{array}{cccc} 0 & n & \cdots & (k-1)n \\ 1 & 1+n & \cdots & 1+(k-1)n \\ \vdots & \vdots & & \vdots \\ n-1 & 2n-1 & \cdots & kn-1 \end{array}$$

- For all $i \in [n]$ and $j \in [k]$,
- the ith row of the jth column is the $i + jn$th position,

Shuffle groups

- For a positive integer m, denote $[m] = \{0, 1, \ldots, m-1\}$.
- k piles:

$$\begin{array}{cccc} 0 & n & \cdots & (k-1)n \\ 1 & 1+n & \cdots & 1+(k-1)n \\ \vdots & \vdots & & \vdots \\ n-1 & 2n-1 & \cdots & kn-1 \end{array}$$

- For all $i \in [n]$ and $j \in [k]$,
- the ith row of the jth column is the $i + jn$th position,
- recall σ and $\rho_\tau \implies (i+jn)^\sigma = ik + j$ and $(i+jn)^{\rho_\tau} = i + j^\tau n$.

Shuffle groups

- For a positive integer m, denote $[m] = \{0, 1, \ldots, m-1\}$.
- k piles:

$$\begin{array}{cccc} 0 & n & \cdots & (k-1)n \\ 1 & 1+n & \cdots & 1+(k-1)n \\ \vdots & \vdots & & \vdots \\ n-1 & 2n-1 & \cdots & kn-1 \end{array}$$

- For all $i \in [n]$ and $j \in [k]$,
- the ith row of the jth column is the $i + jn$th position,
- recall σ and $\rho_\tau \implies (i + jn)^\sigma = ik + j$ and $(i + jn)^{\rho_\tau} = i + j^\tau n$.
- The shuffle group on kn cards, denoted by $G_{k,kn}$, is generated by all possible shuffles $\rho_\tau \sigma$ for $\tau \in \mathrm{Sym}(\{0, \ldots, k-1\})$.

Shuffle groups

- For a positive integer m, denote $[m] = \{0, 1, \ldots, m-1\}$.
- k piles:

$$\begin{array}{cccc} 0 & n & \cdots & (k-1)n \\ 1 & 1+n & \cdots & 1+(k-1)n \\ \vdots & \vdots & & \vdots \\ n-1 & 2n-1 & \cdots & kn-1 \end{array}$$

- For all $i \in [n]$ and $j \in [k]$,
- the ith row of the jth column is the $i + jn$th position,
- recall σ and $\rho_\tau \implies (i+jn)^\sigma = ik + j$ and $(i+jn)^{\rho_\tau} = i + j^\tau n$.
- The shuffle group on kn cards, denoted by $G_{k,kn}$, is generated by all possible shuffles $\rho_\tau\sigma$ for $\tau \in \mathrm{Sym}(\{0, \ldots, k-1\})$. ($G_{k,kn} = \langle \rho_\tau\sigma \mid \tau \in \mathrm{Sym}(k) \rangle = \langle \rho_\tau, \sigma \mid \tau \in \mathrm{Sym}(k) \rangle$.)

Literature on $G_{k,kn}$ for $k \geq 3$

- Medvedoff and Morrison[2] in 1987 conjectured:

---

[2] S. Medvedoff and K. Morrison, Groups of perfect shuffles, *Math. Mag.*, 60 (1987), 3–14.

Literature on $G_{k,kn}$ for $k \geq 3$

- Medvedoff and Morrison[2] in 1987 conjectured:
  - $G_{3,3n} \geq \mathrm{Alt}(3n)$ if n is not a power of 3;

[2] S. Medvedoff and K. Morrison, Groups of perfect shuffles, *Math. Mag.*, 60 (1987), 3–14.

Literature on $G_{k,kn}$ for $k \geq 3$

- Medvedoff and Morrison[2] in 1987 conjectured:
  - $G_{3,3n} \geq \mathrm{Alt}(3n)$ if n is not a power of 3;
  - $G_{4,4n} \geq \mathrm{Alt}(4n)$ if n is not a power of 2;

[2] S. Medvedoff and K. Morrison, Groups of perfect shuffles, *Math. Mag.*, 60 (1987), 3–14.

Literature on $G_{k,kn}$ for $k \geq 3$

- Medvedoff and Morrison[2] in 1987 conjectured:
  - $G_{3,3n} \geq \mathrm{Alt}(3n)$ if n is not a power of 3;
  - $G_{4,4n} \geq \mathrm{Alt}(4n)$ if n is not a power of 2;
  - $G_{4,2^m} = \mathrm{AGL}(m,2) = C_2^m \rtimes \mathrm{GL}(m,2)$ if $m \geq 3$ is odd.

[2] S. Medvedoff and K. Morrison, Groups of perfect shuffles, *Math. Mag.*, 60 (1987), 3–14.

Literature on $G_{k,kn}$ for $k \geq 3$

- Medvedoff and Morrison[2] in 1987 conjectured:
  - $G_{3,3n} \geq \mathrm{Alt}(3n)$ if n is not a power of 3;
  - $G_{4,4n} \geq \mathrm{Alt}(4n)$ if n is not a power of 2;
  - $G_{4,2^m} = \mathrm{AGL}(m,2) = C_2^m \rtimes \mathrm{GL}(m,2)$ if $m \geq 3$ is odd.

- In [2] they also proved:
  - $G_{k,kn} \leq \mathrm{Alt}(kn)$ if and only if either $n \equiv 0 \pmod 4$, or $n \equiv 2 \pmod 4$ and $k \equiv 0$ or $1 \pmod 4$.
  - $G_{k,k^m} = \mathrm{Sym}(k) \wr C_m$.

[2] S. Medvedoff and K. Morrison, Groups of perfect shuffles, *Math. Mag.*, 60 (1987), 3–14.

Literature on $G_{k,kn}$ for $k \geq 3$

- Cohen, Harmse, Morrison and Wright[3] confirmed the latter part of MM's conjecture when $k = 4$.

  ($G_{4,2^m} = \mathrm{AGL}(m, 2)$ for some odd integer $m \geq 3$)

[3] A. Cohen, A. Harmse, K.E. Morrison and S. Wright, Perfect shuffles and affine groups, 2005, https://aimath.org/morrison/Research/shuffles.

Literature on $G_{k,kn}$ for $k \geq 3$

- Cohen, Harmse, Morrison and Wright[3] confirmed the latter part of MM's conjecture when $k = 4$.

  ($G_{4,2^m} = \mathrm{AGL}(m, 2)$ for some odd integer $m \geq 3$)

- In [3] they also posed:

Shuffle Group Conjecture (2005)

For $k \geq 3$, if n is not a power of k and $(k, n) \neq (4, 2^f)$ for any positive integer f, then $G_{k,kn} \geq A_{kn}$.

[3] A. Cohen, A. Harmse, K.E. Morrison and S. Wright, Perfect shuffles and affine groups, 2005, https://aimath.org/morrison/Research/shuffles.

Literature on $G_{k,kn}$ for $k \geq 3$

- Amarra, Morgan and Praeger[4] confirmed the Shuffle Group Conjecture in the following cases:

[4] C. Amarra, L. Morgan and C. Praeger, Generalised shuffle groups, *Israel J. Math.*, 244 (2021), 807–856.

Literature on $G_{k,kn}$ for $k \geq 3$

- Amarra, Morgan and Praeger[4] confirmed the Shuffle Group Conjecture in the following cases:
  - $k > n$;

[4] C. Amarra, L. Morgan and C. Praeger, Generalised shuffle groups, *Israel J. Math.*, 244 (2021), 807–856.

Literature on $G_{k,kn}$ for $k \geq 3$

- Amarra, Morgan and Praeger[4] confirmed the Shuffle Group Conjecture in the following cases:
  - $k > n$;
  - k and n are powers of the same integer $\ell \geq 2$;

[4] C. Amarra, L. Morgan and C. Praeger, Generalised shuffle groups, *Israel J. Math.*, 244 (2021), 807–856.

Literature on $G_{k,kn}$ for $k \geq 3$

- Amarra, Morgan and Praeger[4] confirmed the Shuffle Group Conjecture in the following cases:
  - $k > n$;
  - k and n are powers of the same integer $\ell \geq 2$;
  - k is a power of 2.

[4] C. Amarra, L. Morgan and C. Praeger, Generalised shuffle groups, *Israel J. Math.*, 244 (2021), 807–856.

Literature on $G_{k,kn}$ for $k \geq 3$

- Amarra, Morgan and Praeger[4] confirmed the Shuffle Group Conjecture in the following cases:
  - $k > n$;
  - k and n are powers of the same integer $\ell \geq 2$;
  - k is a power of 2.
- In [4] they also opened up the study of “generalized shuffle groups".

[4] C. Amarra, L. Morgan and C. Praeger, Generalised shuffle groups, *Israel J. Math.*, 244 (2021), 807–856.

Our contribution

Theorem (Xia-Zhang-Z. 2023^{+})

The Shuffle Group Conjecture holds when $k \geq 4$ or k does not divide n.

Our contribution

Theorem (Xia-Zhang-Z. 2023^+)

The Shuffle Group Conjecture holds when $k \geq 4$ or k does not divide n.

We established two key lemmas to prove the theorem.

Our contribution

Theorem (Xia-Zhang-Z. 2023^+)

The Shuffle Group Conjecture holds when $k \geq 4$ or k does not divide n.

We established two key lemmas to prove the theorem.

- Reduction Lemma: If $G_{k,kn}$ is 2-transitive, then either $k = 4$ and n is a power of 2, or $G_{k,kn}$ contains A_{kn}.
- 2-transitivity Lemma: If either $k \geq 4$ and n is not a power of k, or $k = 3$ and n is not divisible by 3, then $G_{k,kn}$ is 2-transitive.

Our contribution

Theorem (Xia-Zhang-Z. 2023^+)

The Shuffle Group Conjecture holds when $k \geq 4$ or k does not divide n.

We established two key lemmas to prove the theorem.

- Reduction Lemma: If $G_{k,kn}$ is 2-transitive, then either $k = 4$ and n is a power of 2, or $G_{k,kn}$ contains A_{kn}.
- 2-transitivity Lemma: If either $k \geq 4$ and n is not a power of k, or $k = 3$ and n is not divisible by 3, then $G_{k,kn}$ is 2-transitive.
- A permutation group G on a set Ω is said to be 2-transitive if the induced action of G on $\Omega \times \Omega \setminus \{(\alpha, \alpha) \mid \alpha \in \Omega\}$ is transitive.

Reducing to 2-transitivity

Reduction Lemma (Xia-Zhang-Z. 2023^{+})

If $G_{k,kn}$ is 2-transitive, then either $k = 4$ and n is a power of 2, or $G_{k,kn}$ contains A_{kn}.

Reducing to 2-transitivity

Reduction Lemma (Xia-Zhang-Z. 2023^+)

If $G_{k,kn}$ is 2-transitive, then either $k = 4$ and n is a power of 2, or $G_{k,kn}$ contains A_{kn}.

- The proof is by examining the list of 2-transitive groups for elements of large fixed point ratio.

Reducing to 2-transitivity

Reduction Lemma (Xia-Zhang-Z. 2023^+)

If $G_{k,kn}$ is 2-transitive, then either $k = 4$ and n is a power of 2, or $G_{k,kn}$ contains A_{kn}.

- The proof is by examining the list of 2-transitive groups for elements of large fixed point ratio.
- The fixed point ratio of a permutation g on a finite set Ω, denoted by $\mathrm{fpr}(g)$, is defined as $\mathrm{fpr}(g) = |\mathrm{Fix}(g)|/|\Omega|$, where $\mathrm{Fix}(g) = \{\alpha \in \Omega \mid \alpha^g = \alpha\}$.

Reducing to 2-transitivity

Reduction Lemma (Xia-Zhang-Z. 2023^+)

If $G_{k,kn}$ is 2-transitive, then either $k = 4$ and n is a power of 2, or $G_{k,kn}$ contains A_{kn}.

- The proof is by examining the list of 2-transitive groups for elements of large fixed point ratio.
- The fixed point ratio of a permutation g on a finite set Ω, denoted by $\mathrm{fpr}(g)$, is defined as $\mathrm{fpr}(g) = |\mathrm{Fix}(g)|/|\Omega|$, where $\mathrm{Fix}(g) = \{\alpha \in \Omega \mid \alpha^g = \alpha\}$.
- Observation: $\mathrm{fpr}(\rho_\tau) = \mathrm{fpr}(\tau)$

Reducing to 2-transitivity

Reduction Lemma (Xia-Zhang-Z. 2023$^+$)

If $G_{k,kn}$ is 2-transitive, then either $k = 4$ and n is a power of 2, or $G_{k,kn}$ contains A_{kn}.

- The proof is by examining the list of 2-transitive groups for elements of large fixed point ratio.
- The fixed point ratio of a permutation g on a finite set Ω, denoted by $\mathrm{fpr}(g)$, is defined as $\mathrm{fpr}(g) = |\mathrm{Fix}(g)|/|\Omega|$, where $\mathrm{Fix}(g) = \{\alpha \in \Omega \mid \alpha^g = \alpha\}$.
- Observation: $\mathrm{fpr}(\rho_\tau) = \mathrm{fpr}(\tau) \Longrightarrow \mathrm{fpr}(\rho_\tau) = (k-2)/k$ when τ is a transposition.

An example of the examination

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d, p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d,p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

- Recall the observation: $\exists\ \rho_\tau \in G$ s.t. $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d, p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

- Recall the observation: $\exists\ \rho_\tau \in G$ s.t. $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.
- G is transitive $\Longrightarrow$ we may assume $\rho_\tau \in G_0 \leq \mathrm{GL}(V)$.

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d, p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

- Recall the observation: $\exists\ \rho_\tau \in G$ s.t. $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.
- G is transitive $\Longrightarrow$ we may assume $\rho_\tau \in G_0 \leq \mathrm{GL}(V)$.
- $\mathrm{fpr}(\rho_\tau) = |\{v \in V \mid v^{\rho_\tau} = v\}|/|V| = p^f/p^d = 1/p^{d-f}$.

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d, p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

- Recall the observation: $\exists\ \rho_\tau \in G$ s.t. $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.
- G is transitive $\Longrightarrow$ we may assume $\rho_\tau \in G_0 \leq \mathrm{GL}(V)$.
- $\mathrm{fpr}(\rho_\tau) = |\{v \in V \mid v^{\rho_\tau} = v\}|/|V| = p^f/p^d = 1/p^{d-f}$.
- $(k-2)/k = 1/p^{d-f}$

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d,p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

- Recall the observation: $\exists\ \rho_\tau \in G$ s.t. $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.
- G is transitive $\Longrightarrow$ we may assume $\rho_\tau \in G_0 \leq \mathrm{GL}(V)$.
- $\mathrm{fpr}(\rho_\tau) = |\{v \in V \mid v^{\rho_\tau} = v\}|/|V| = p^f/p^d = 1/p^{d-f}$.
- $(k-2)/k = 1/p^{d-f} \Longrightarrow (k,p)$ is either $(3,3)$ or $(4,2)$.

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d,p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

- Recall the observation: $\exists\ \rho_\tau \in G$ s.t. $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.
- G is transitive $\Longrightarrow$ we may assume $\rho_\tau \in G_0 \leq \mathrm{GL}(V)$.
- $\mathrm{fpr}(\rho_\tau) = |\{v \in V \mid v^{\rho_\tau} = v\}|/|V| = p^f/p^d = 1/p^{d-f}$.
- $(k-2)/k = 1/p^{d-f} \Longrightarrow (k,p)$ is either $(3,3)$ or $(4,2)$.
- $kn = |V| = p^d \Longrightarrow (k,n)$ is either $(3, 3^{d-1})$ or $(4, 2^{d-2})$.

An example of the examination

Write $G = G_{k,kn}$. Suppose G is an affine 2-transitive permutation group, i.e., $G \leq \mathrm{AGL}(V) = \mathrm{AGL}(d,p)$ for some d-dimension vector space V over a prime field $\mathbb{F}_p$.

- Recall the observation: $\exists\ \rho_\tau \in G$ s.t. $\mathrm{fpr}(\rho_\tau) = (k-2)/k$.
- G is transitive $\Longrightarrow$ we may assume $\rho_\tau \in G_0 \leq \mathrm{GL}(V)$.
- $\mathrm{fpr}(\rho_\tau) = |\{v \in V \mid v^{\rho_\tau} = v\}|/|V| = p^f/p^d = 1/p^{d-f}$.
- $(k-2)/k = 1/p^{d-f} \Longrightarrow (k,p)$ is either $(3,3)$ or $(4,2)$.
- $kn = |V| = p^d \Longrightarrow (k,n)$ is either $(3, 3^{d-1})$ or $(4, 2^{d-2})$.
- Note that $G_{3,3^d}$ and $G_{4,2^d}$ have been determined.

2-transitivity of $G_{k,kn}$

2-transitivity Lemma (Xia-Zhang-Z. 2023^{+})

If either $k \geq 4$ and n is not a power of k, or $k = 3$ and n is not divisible by 3, then $G_{k,kn}$ is 2-transitive.

2-transitivity of $G_{k,kn}$

2-transitivity Lemma (Xia-Zhang-Z. 2023^+)

If either $k \geq 4$ and n is not a power of k, or $k = 3$ and n is not divisible by 3, then $G_{k,kn}$ is 2-transitive.

- The proof of this lemma is combinatorial in nature.

2-transitivity of $G_{k,kn}$

2-transitivity Lemma (Xia-Zhang-Z. 2023^+)

If either $k \geq 4$ and n is not a power of k, or $k = 3$ and n is not divisible by 3, then $G_{k,kn}$ is 2-transitive.

- The proof of this lemma is combinatorial in nature.
- Shuffle Group Conjecture $\xrightarrow{\textit{Reduction Lemma}}$ 2-transitivity of $G_{k,kn}$.

2-transitivity of $G_{k,kn}$

2-transitivity Lemma (Xia-Zhang-Z. 2023$^+$)

If either $k \geq 4$ and n is not a power of k, or $k = 3$ and n is not divisible by 3, then $G_{k,kn}$ is 2-transitive.

- The proof of this lemma is combinatorial in nature.
- Shuffle Group Conjecture $\xrightarrow{\textit{Reduction Lemma}}$ 2-transitivity of $G_{k,kn}$.
- Thus the remaining unresolved case of the conjecture is that $k = 3$ divides n.

Sketch of Proof to 2-transitivity Lemma

- Let $G = G_{k,kn}$ and $[m] = \{0, 1, \ldots, m-1\}$.

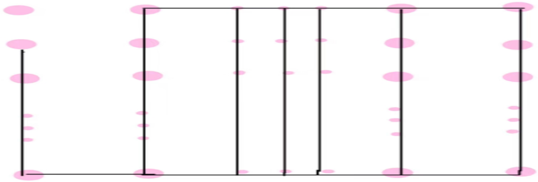
Sketch of Proof to 2-transitivity Lemma

- Let $G = G_{k,kn}$ and $[m] = \{0, 1, \ldots, m-1\}$.

- G is 2-transitive on $[kn]$ iff G_0 is transitive on $[m] \backslash \{0\}$.

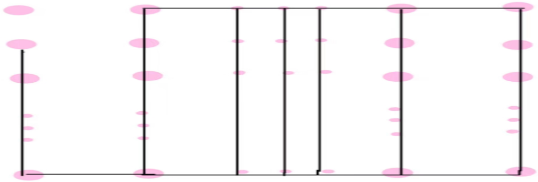
Sketch of Proof to 2-transitivity Lemma

- Let $G = G_{k,kn}$ and $[m] = \{0, 1, \ldots, m-1\}$.
- G is 2-transitive on $[kn]$ iff G_0 is transitive on $[m]\backslash\{0\}$.



Sketch of Proof to 2-transitivity Lemma

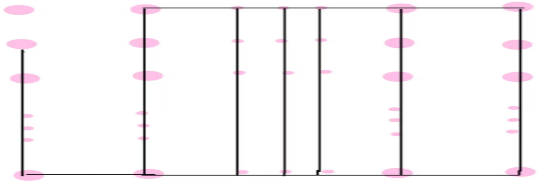
- Let $G = G_{k,kn}$ and $[m] = \{0, 1, \ldots, m-1\}$.
- G is 2-transitive on $[kn]$ iff G_0 is transitive on $[m] \backslash \{0\}$.



- we complete this proof through the following cases:

Sketch of Proof to 2-transitivity Lemma

- Let $G = G_{k,kn}$ and $[m] = \{0, 1, \ldots, m-1\}$.
- G is 2-transitive on $[kn]$ iff G_0 is transitive on $[m]\backslash\{0\}$.



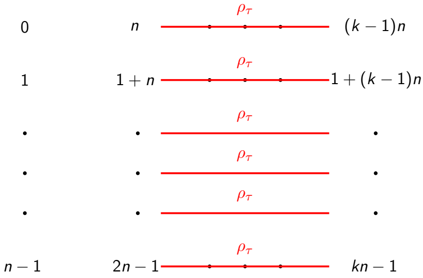
- we complete this proof through the following cases:
  - $k \nmid n$ with $k \geq 4$; (only elaborate on this case here)
  - $k \nmid n$ with $k = 3$;
  - $k \mid n$ with $k \geq 4$.

Case for $k \nmid n$ with $k \geq 4$

$$\begin{array}{cccccc}
0 & n & \cdot & \cdot & \cdot & (k-1)n \\
1 & 1+n & \cdot & \cdot & \cdot & 1+(k-1)n \\
\cdot & \cdot & & & & \cdot \\
\cdot & \cdot & & & & \cdot \\
\cdot & \cdot & & & & \cdot \\
n-1 & 2n-1 & \cdot & \cdot & \cdot & kn-1
\end{array}$$

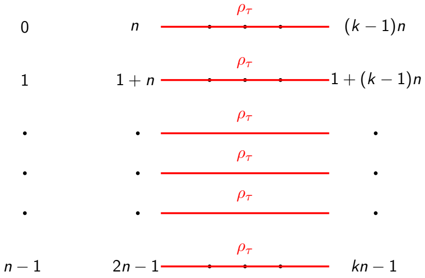
- $(i+jn)^{\rho_\tau} = i + j^\tau n$;

Case for $k \nmid n$ with $k \geq 4$



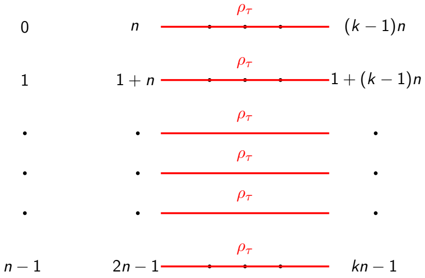
- $(i + jn)^{\rho_\tau} = i + j^\tau n$;

Case for $k \nmid n$ with $k \geq 4$



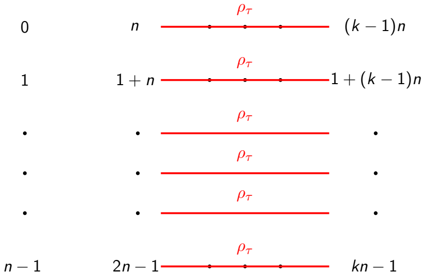
- $(i + jn)^{\rho_\tau} = i + j^\tau n$;
- recall $(i + jn)^\sigma = ik + j$;

Case for $k \nmid n$ with $k \geq 4$



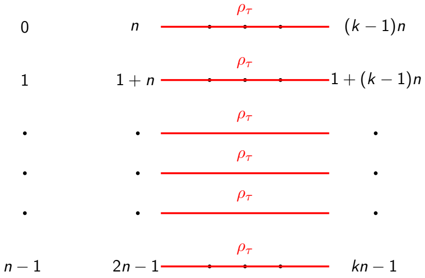
- $(i + jn)^{\rho_\tau} = i + j^\tau n$;
- recall $(i + jn)^\sigma = ik + j$;
- $(ik + 1)^{\sigma^{-1}\rho_\tau\sigma} = (i + 1 \cdot n)^{\rho_\tau\sigma} = (i + 1^\tau \cdot n)^\sigma = ik + 1^\tau$

Case for $k \nmid n$ with $k \geq 4$



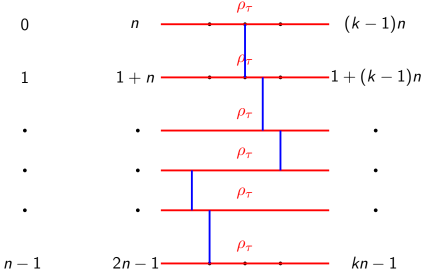
- $(i+jn)^{\rho_\tau} = i + j^\tau n$;
- recall $(i+jn)^\sigma = ik + j$;
- $(ik+1)^{\sigma^{-1}\rho_\tau\sigma} = (i+1\cdot n)^{\rho_\tau\sigma} = (i+1^\tau \cdot n)^\sigma = ik + 1^\tau$
  $\implies \{ik+1, ik+2\ldots, ik+k-1\}$ in the same orbit of G_0.

Case for $k \nmid n$ with $k \geq 4$



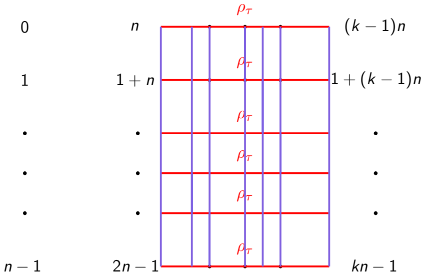
- $(i+jn)^{\rho_\tau} = i + j^\tau n$;
- recall $(i+jn)^\sigma = ik + j$;
- $(ik+1)^{\sigma^{-1}\rho_\tau\sigma} = (i+1\cdot n)^{\rho_\tau\sigma} = (i+1^\tau\cdot n)^\sigma = ik+1^\tau$
  $\Longrightarrow \{ik+1, ik+2\ldots, ik+k-1\}$ in the same orbit of G_0.
- $k \geq 4$ and $k \nmid n$

Case for $k \nmid n$ with $k \geq 4$



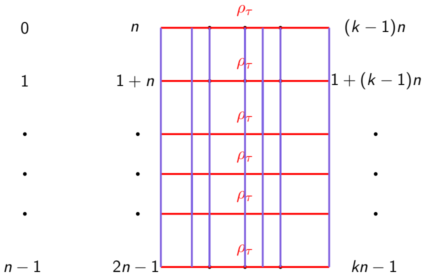
- $(i+jn)^{\rho_\tau} = i + j^\tau n$;
- recall $(i+jn)^\sigma = ik + j$;
- $(ik+1)^{\sigma^{-1}\rho_\tau\sigma} = (i+1\cdot n)^{\rho_\tau\sigma} = (i+1^\tau \cdot n)^\sigma = ik + 1^\tau$
  $\Longrightarrow \{ik+1, ik+2\ldots, ik+k-1\}$ in the same orbit of G_0.
- $k \geq 4$ and $k \nmid n \implies$ for $\forall\ x \in [n]$, $\exists\ y \in \{x+n, x+2n, x+3n\}$ s.t. $y \sim y+1$.

Case for $k \nmid n$ with $k \geq 4$



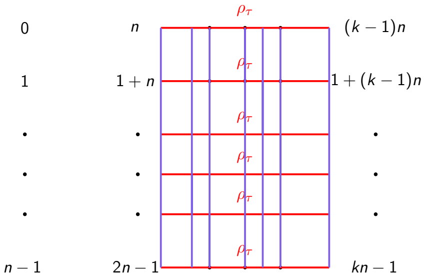
- $(i + jn)^{\rho_\tau} = i + j^\tau n$;
- recall $(i + jn)^\sigma = ik + j$;
- $(ik + 1)^{\sigma^{-1}\rho_\tau\sigma} = (i + 1 \cdot n)^{\rho_\tau\sigma} = (i + 1^\tau \cdot n)^\sigma = ik + 1^\tau$
  $\Longrightarrow \{ik + 1, ik + 2 \ldots, ik + k - 1\}$ in the same orbit of G_0.
- $k \geq 4$ and $k \nmid n \Longrightarrow$ for $\forall\ x \in [n]$, $\exists\ y \in \{x + n, x + 2n, x + 3n\}$ s.t. $y \sim y + 1$.

Case for $k \nmid n$ with $k \geq 4$



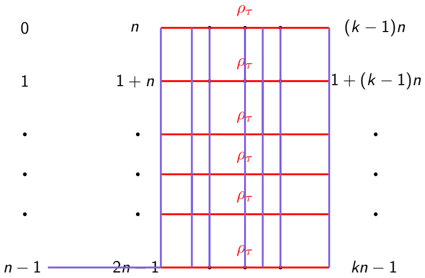
- $x^\sigma \equiv kx \pmod{kn-1}$ for all $x \in [kn]$;

Case for $k \nmid n$ with $k \geq 4$



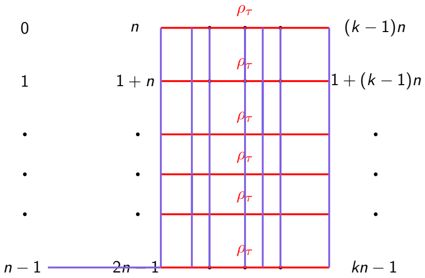
- $x^\sigma \equiv kx \pmod{kn-1}$ for all $x \in [kn]$;
- $(n-1)^\sigma = k(n-1)$

Case for $k \nmid n$ with $k \geq 4$



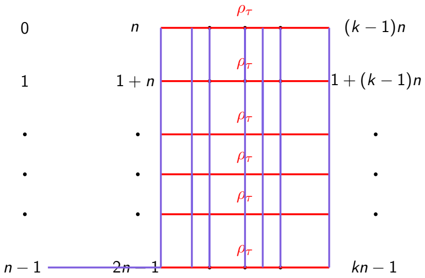
- $x^\sigma \equiv kx \pmod{kn-1}$ for all $x \in [kn]$;
- $(n-1)^\sigma = k(n-1) \xrightarrow{n-1<(n-1)k<kn-1} n-1 \in n^{G_0}$;

Case for $k \nmid n$ with $k \geq 4$



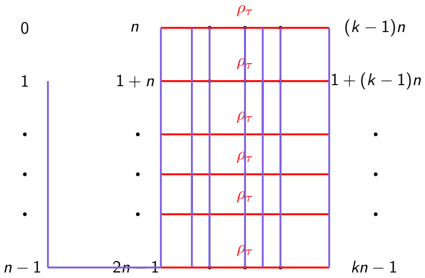
- $x^\sigma \equiv kx \pmod{kn-1}$ for all $x \in [kn]$;
- $(n-1)^\sigma = k(n-1) \xrightarrow{n-1<(n-1)k<kn-1} n-1 \in n^{G_0}$;
- suppose $\exists\ x \in [n-1] \backslash \{0\}$ s.t $y \in n^{G_0}$ for all $y > x$.

Case for $k \nmid n$ with $k \geq 4$



- $x^\sigma \equiv kx \pmod{kn-1}$ for all $x \in [kn]$;
- $(n-1)^\sigma = k(n-1) \xrightarrow{n-1<(n-1)k<kn-1} n-1 \in n^{G_0}$;
- suppose $\exists\ x \in [n-1] \backslash \{0\}$ s.t $y \in n^{G_0}$ for all $y > x$.
- $x^\sigma = kx > x$

Case for $k \nmid n$ with $k \geq 4$



- $x^\sigma \equiv kx \pmod{kn-1}$ for all $x \in [kn]$;
- $(n-1)^\sigma = k(n-1) \xrightarrow{n-1<(n-1)k<kn-1} n-1 \in n^{G_0}$;
- suppose $\exists\ x \in [n-1]\backslash\{0\}$ s.t $y \in n^{G_0}$ for all $y > x$.
- $x^\sigma = kx > x \implies x \in n^{G_0}$.

Thank you for listening!