Card Shuffle Groups

Zhishuo Zhang

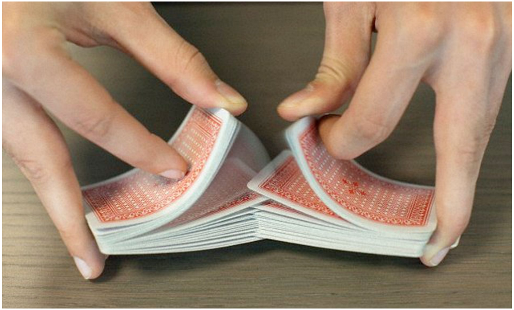
The University of Melbourne

Joint work with Binzhou Xia, Junyang Zhang and Wenying Zhu.

December 11, 2023

Shuffle Cards

We are motivated by an interesting paper[1] about mathematics in shuffling cards.



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

Perfect Shuffle

- Cut the deck in half:

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

- perfectly interleave them:

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

Out-shuffle O In-shuffle I

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, since $O \in \mathrm{Sym}(52)$

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

Answer: 8 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, since $O \in \mathrm{Sym}(52)$

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

Answer: 8 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, since $O \in \mathrm{Sym}(52)$

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

Answer: 8 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, since $O \in \mathrm{Sym}(52)$

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

Answer: 8 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, since $O \in \mathrm{Sym}(52)$

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

Answer: 8 times.

More patterns

- The order of the $2n$ cards after O is

$$(0, n, 1, n+1, \ldots, n-1, 2n-1).$$

$\Longrightarrow$ The inversion number of O is
$1 + \cdots + n - 1 = n(n-1)/2$.
$\Longrightarrow$ O is even iff $n \equiv 0$ or $1 \pmod 4$.

- I is obtained by permutating the two piles and then performing O. $\Longrightarrow$ I is even iff n and O have the same parity.
$\Longrightarrow$ I is even iff $n \equiv 0$ or $3 \pmod 4$.

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

$\langle O, I \rangle \longleftrightarrow$all the orderings by performing a sequence of Out-shuffles and In-shuffles

More patterns

- The order of the $2n$ cards after O is
$$(0, n, 1, n+1, \ldots, n-1, 2n-1).$$
$\Longrightarrow$ The inversion number of O is $1 + \cdots + n - 1 = n(n-1)/2$.
$\Longrightarrow$ O is even iff $n \equiv 0 \text{ or } 1 \pmod 4$.

- I is obtained by permutating the two piles and then performing O. $\Longrightarrow$ I is even iff n and O have the same parity.
$\Longrightarrow$ I is even iff $n \equiv 0 \text{ or } 3 \pmod 4$.

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

$\langle O, I \rangle \longleftrightarrow$all the orderings by performing a sequence of Out-shuffles and In-shuffles

More patterns

- The order of the $2n$ cards after O is
$$(0, n, 1, n+1, \dots, n-1, 2n-1).$$
$\Longrightarrow$ The inversion number of O is
$1 + \cdots + n - 1 = n(n-1)/2$.
$\Longrightarrow$ O is even iff $n \equiv 0$ or $1 \pmod 4$.

- I is obtained by permutating the two piles and then performing O. $\Longrightarrow$ I is even iff n and O have the same parity.
$\Longrightarrow$ I is even iff $n \equiv 0$ or $3 \pmod 4$.

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

$\langle O, I\rangle \longleftrightarrow$ all the orderings by performing a sequence of Out-shuffles and In-shuffles

More patterns

- The order of the $2n$ cards after O is
$$(0, n, 1, n+1, \dots, n-1, 2n-1).$$
$\Longrightarrow$ The inversion number of O is $1 + \cdots + n - 1 = n(n-1)/2$.
$\Longrightarrow$ O is even iff $n \equiv 0 \text{ or } 1 \pmod 4$.

- I is obtained by permutating the two piles and then performing O. $\Longrightarrow$ I is even iff n and O have the same parity.
$\Longrightarrow$ I is even iff $n \equiv 0 \text{ or } 3 \pmod 4$.

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

$\langle O, I \rangle \longleftrightarrow$all the orderings by performing a sequence of Out-shuffles and In-shuffles

More patterns

- The order of the $2n$ cards after O is

$$(0, n, 1, n+1, \ldots, n-1, 2n-1).$$

  $\Longrightarrow$ The inversion number of O is $1 + \cdots + n - 1 = n(n-1)/2$.
  $\Longrightarrow$ O is even iff $n \equiv 0$ or $1 \pmod 4$.

- I is obtained by permutating the two piles and then performing O. $\Longrightarrow$ I is even iff n and O have the same parity.
  $\Longrightarrow$ I is even iff $n \equiv 0$ or $3 \pmod 4$.

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

$\langle O, I \rangle \longleftrightarrow$ all the orderings by performing a sequence of Out-shuffles and In-shuffles

More patterns

- The order of the $2n$ cards after O is

$$(0, n, 1, n+1, \ldots, n-1, 2n-1).$$

$\implies$ The inversion number of O is
$1 + \cdots + n - 1 = n(n-1)/2$.
$\implies$ O is even iff $n \equiv 0$ or $1 \pmod 4$.

- I is obtained by permutating the two piles and then performing O. $\implies$ I is even iff n and O have the same parity.
$\implies$ I is even iff $n \equiv 0$ or $3 \pmod 4$.

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

$\langle O, I \rangle \longleftrightarrow$ all the orderings by performing a sequence of Out-shuffles and In-shuffles

More patterns

- The order of the $2n$ cards after O is

$$(0, n, 1, n+1, \ldots, n-1, 2n-1).$$

$\Longrightarrow$ The inversion number of O is
$1 + \cdots + n - 1 = n(n-1)/2$.
$\Longrightarrow$ O is even iff $n \equiv 0$ or $1 \pmod 4$.

- I is obtained by permutating the two piles and then performing O. $\Longrightarrow$ I is even iff n and O have the same parity.
$\Longrightarrow$ I is even iff $n \equiv 0$ or $3 \pmod 4$.

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

$\langle O, I \rangle \longleftrightarrow$all the orderings by performing a sequence of Out-shuffles and In-shuffles

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: out-shuffle and in-shuffle preserve the partition $\{0, 2n-1\}, \{1, 2n-2\}, \dots, \{n-1, n\}$.

Question

What is the goup structure of $\langle O, I \rangle$?

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

Question

What is the goup structure of $\langle O, I \rangle$?

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

Question

What is the goup structure of $\langle O, I \rangle$?

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

Question

What is the goup structure of $\langle O, I \rangle$?

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: out-shuffle and in-shuffle preserve the partition $\{0, 2n-1\}, \{1, 2n-2\}, \dots, \{n-1, n\}$.

Question

What is the goup structure of $\langle O, I \rangle$?

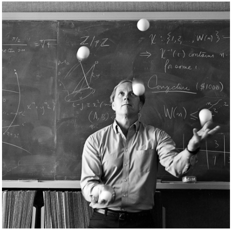
Diaconis-Graham-Kantor

Question: What is the goup structure of $\langle O, I \rangle$?

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.

Structures of $\langle O, I \rangle$

Size of each pile n	$\langle O, I \rangle$
$n \equiv 0 \pmod 4$, $n > 12$ 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 $n > 6$	$C_2 \wr S_n$
$n \equiv 3 \pmod 4$	$C_2^{n-1} \rtimes S_n$
$n = 2^f$ for some positive integer f	$C_2 \wr C_{f+1}$
$n = 6$	$C_2^6 \rtimes \mathrm{PGL}(2,5)$
$n = 12$	$C_2^{11} \rtimes M_{12}$

Table: Classification of $\langle O, I \rangle$

C_2^n: direct product of n copies of cyclic groups of order 2.
M_{12}: the sporadic Mathieu group on 12 points.

[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).

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

- Standard shuffle σ: $(i+jn)^\sigma = ik+j$.
- ρ_τ: $(i+jn)^{\rho_\tau} = i + j^\tau n$.
- The shuffle group on kn cards, denoted by $G_{k,kn}$, is generated by all possible shuffles $\rho_\tau \sigma$ for $\tau \in \mathrm{Sym}(\{0,\ldots,k-1\})$.
  $G_{k,kn} = \langle \rho_\tau \sigma \mid \tau \in \mathrm{Sym}(k) \rangle = \langle \rho_\tau, \sigma \mid \tau \in \mathrm{Sym}(k) \rangle$.

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: $(i + jn)^\sigma = ik + j$.
- ρ_τ: $(i + jn)^{\rho_\tau} = i + j^\tau n$.
- 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:
  - $G_{3,3n} \geq \mathrm{Alt}(3n)$ 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 $m \geq 3$)

- 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:
  - $k > n$;
  - k and n are powers of the same integer $\ell \geq 2$;
  - k is a power of 2.
- 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

We confirmed Shuffle Group Conjecture for all the left cases.

Theorem

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 $G_{k,kn} \geq A_{kn}$.

This thoerem leads to a complete classification of shuffle groups.

Our contribution

We confirmed Shuffle Group Conjecture for all the left cases.

Theorem

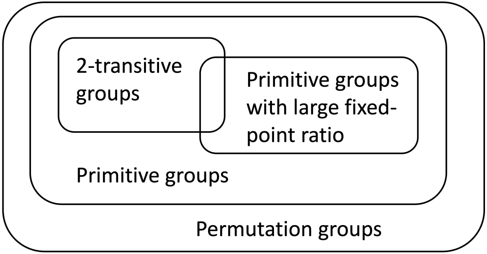
For $k \geq 3$, if n is not a power of k and $(k, n) \neq (4, 2^f)$ for any positive integer f, then $G_{k,kn} \geq A_{kn}$.

This thoerem leads to a complete classification of shuffle groups.

Outline of the proof

Prove: $G_{k,kn} = A_{kn}$ or S_{kn}, where $k \geqslant 3$, n is not a power of k and $(k, n) \neq (4, 2^f)$ for any positive integer f.

- $G_{k,kn}$ is 2-transitive.
- $G_{k,kn}$ has an element with large fixed-point ratio.
- classification of 2-transitive groups and primitive groups with large fixed-point ratio.
- Exclude all the candidates except from A_{kn} and S_{kn}.



2-transitivity

- $G_{k,kn}$ is 2-transitive iff its stabilizer on the point $kn-1$, denoted by H, is transitive on $\{0,\dots,kn-2\}$.
- In the proof of $G_{k,k^m} = S_k \wr C_m$, they found patterns by writing numbers $\{0,\dots,kn-2\}$ in base k.
- Let $n = k^s t$, where $k \nmid t$ and $t > 1$. Write
$$x = (x_s k^s + \cdots + x_1 k + x_0)t + X.$$
We have a bijection
$$x \longleftrightarrow (x_s,\dots,x_1,x_0;X).$$
- Find an inductive index $T(x) = |\{i \mid x_i = k-1\}|$.
- If $T(x) = 0$ then $x \in 0^H$. If $T(x) > 0$, then there eixsts $y \in x^H$ such that $T(y) < T(x)$.