

Kirk Lecture: The Mathematics of Shuffling

Joint work with Carmen Amarra
and Luke Morgan

Cheryl E
Praeger

Centre for the Mathematics of
Symmetry and Computation

Isaac Newton Institute
Cambridge, 17 March
2020

Describe some of the mathematics of shuffling cards

Focus on “perfect shuffles”

- Where the questions came from
- Early work by Diaconis, Graham and Kantor
- New work joint with Carmen Amarra and Luke Morgan



Perfect Shuffles

A deck containing $2n$ cards:

- Cut into two piles of n cards each
- Perfectly interleave them

Two different ways to do this:

Out – shuffle keeps top card on top



Starting order: $(0,1,2,3,4,5,6,7,8,9,10,11)$ ($n = 6$)

Picking up: card 0, then card 6, then card 1, then card 7 and so on

After the out – shuffle: $(0,6,1,7,2,8,3,9,4,10,5,11)$ (top card stays on top)

Perfect Shuffles

A deck containing $2n$ cards:

- Cut into two piles of n cards each
- Perfectly interleave them

Two different ways to do this:

In – shuffle pick up first from the 2nd pile



Starting order: $(0,1,2,3,4,5,6,7,8,9,10,11)$ ($n = 6$)

Picking up: card 6, then card 0, then card 7, then card 1 and so on

After the in – shuffle: $(6,0,7,1,8,2,9,3,10,4,11,5)$

Perfect Shuffles

A deck containing $2n$ cards:

- Cut into two piles of n cards each
- Perfectly interleave them

Out – shuffles and in - shuffles



Questions (**from card players and mathematicians**):

- Can I get card 0 into any chosen position by repeated out or in shuffles?
- How many shuffles to get to a preferred ordering? Or the original order?
- How to alternate these shuffles to “randomize” the order?
- **How many different orderings** are possible?
- **What kind of maths is going on?**

Perfect Shuffles

A deck containing $2n$ cards:

- Cut into two piles of n cards each
- Perfectly interleave them

**Any sequence of in-shuffles and out-shuffles
is a “valid move”**



Interpret as permutations of $2n$ cards: first the out-shuffle

Starting order: $(0,1,2,3,4,5,6,7,8,9,10,11)$

After the out – shuffle: $(0,6,1,7,2,8,3,9,4,10,5,11)$

Interpret as: $(0)(1, 2, 4, 8, 5, 10, 9, 7, 3, 6) (11)$

Perfect Shuffles

A deck containing $2n$ cards:

- Cut into two piles of n cards each
- Perfectly interleave them

**Any sequence of in-shuffles and out-shuffles
is a “valid move”**



Interpret as permutations of $2n$ cards: and the in-shuffle

Starting order: $(0,1,2,3,4,5,6,7,8,9,10,11)$

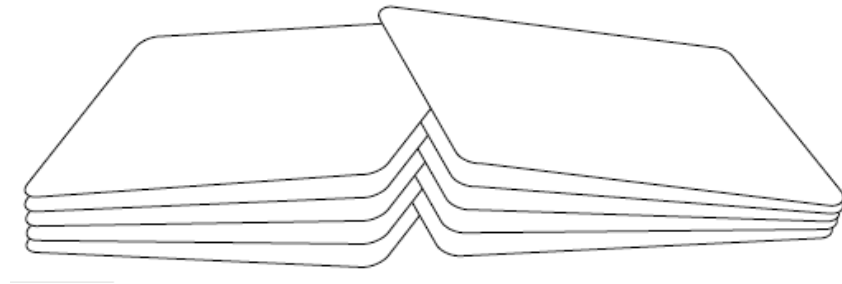
After the in- shuffle: $(6,0,7,1,8,2,9,3,10,4,11,5)$

Interpret in-shuffle as: $(0, 1, 3, 7, 2, 5, 11, 10, 8, 4, 9, 6)$

Quite different from the out-shuffle: $(0)(1, 2, 4, 8, 5, 10, 9, 7, 3, 6) (11)$

What is a shuffle group?

Shuffle group is the set of all permutations obtained by performing any sequence of (any length of) in- and out-shuffles



Shuffles: permutations of the numbers $\{0, 1, 2, \dots, 2n - 1\}$
elements of the **symmetric group** $Sym(2n)$ of all permutations

Shuffle group subgroup of $Sym(2n)$ generated by the out- and in-shuffle.

How big is the shuffle group? What do we know about its structure?
Does it depend on n , and if so how?

1983 Diaconis, Graham and Kantor

“The mathematics of perfect shuffles” Advances in App. Math



- Explain they're not the first – Section 3 gives overview of earlier work:
- Alex Elimsley 1957: importance of $o(2, \text{mod } 2n - 1)$
- Golomb 1961, deck of $2n-1$ cards: Group order is $(2n - 1) \times o(2, \text{mod } 2n - 1)$
- Discuss applications to parallel processing algorithms (Section 4)

And they work out the shuffle groups!

1983 Diaconis, Graham and Kantor

Very technical description – probably meaningless to most everyone

Write $\sigma = 0$ and $\delta = \text{swap the piles}$, so $I = \delta \circ \sigma$ and shuffle group is $\langle \sigma, \delta \rangle$,

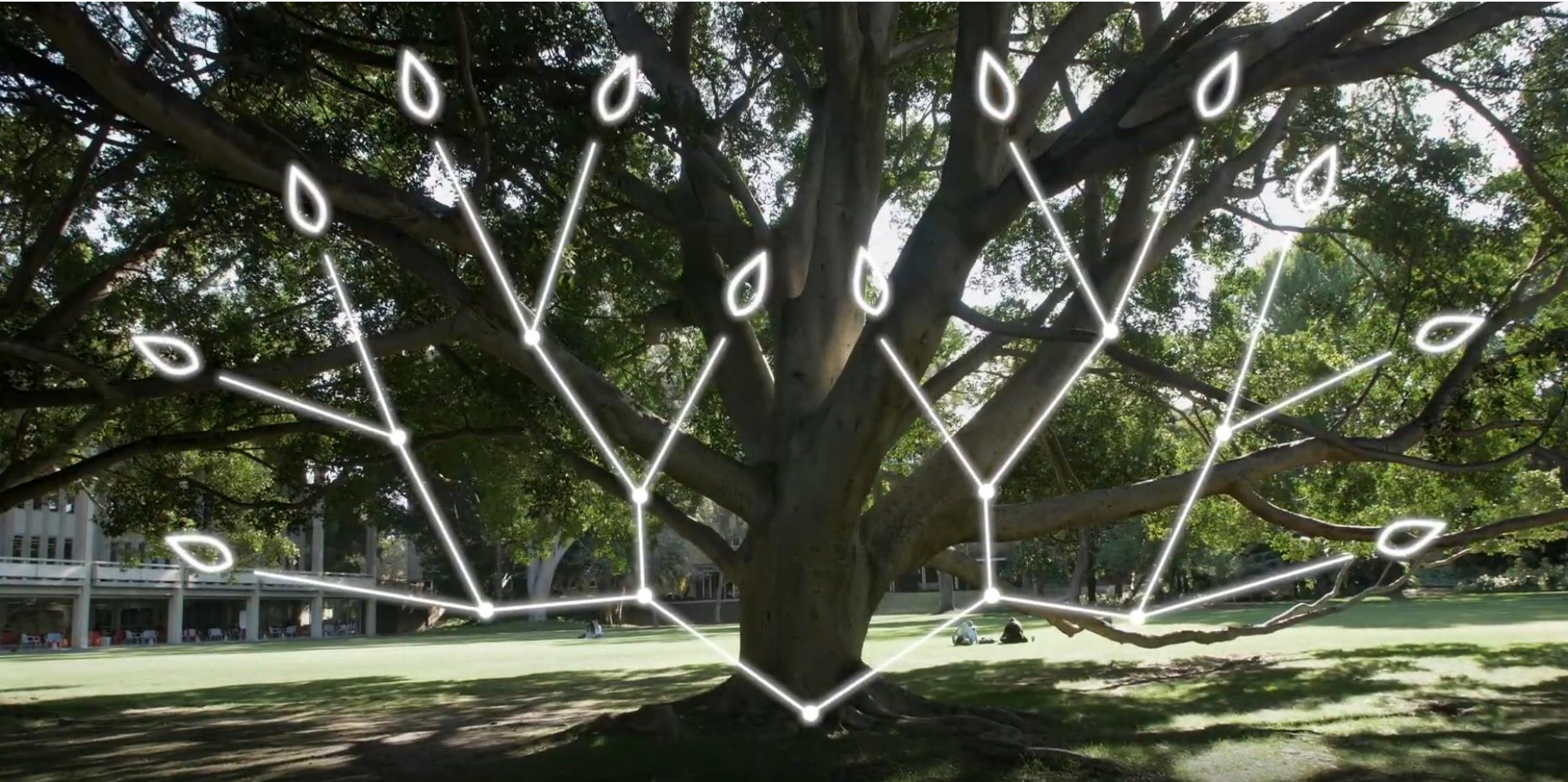
Theorem 1.1. [8, Theorem 1] *The structure of the shuffle group $\langle \sigma, \delta \rangle$ on $2n$ points, where $n \geq 2$, is given in Table 1.*

Size of each pile n	Shuffle group $\langle \sigma, \delta \rangle$
$n = 2^f$ for some positive integer f	$C_2 \wr C_{f+1}$
$n \equiv 0 \pmod{4}$, $n \geq 20$ and n is not a power of 2	$\ker(\text{sgn}) \cap \ker(\overline{\text{sgn}})$
$n \equiv 1 \pmod{4}$ and $n \geq 5$	$\ker(\overline{\text{sgn}})$
$n \equiv 2 \pmod{4}$ and $n \geq 10$	B_n
$n \equiv 3 \pmod{4}$	$\ker(\text{sgn}\overline{\text{sgn}})$
$n = 6$	$C_2^6 \rtimes \text{PGL}(2, 5)$
$n = 12$	$C_2^{11} \rtimes M_{12}$

TABLE 1. The shuffle group on $2n$ points

- $B_n = C_2 \wr \text{Sym}(n) \leq \text{Sym}(2n)$, for $g \in B_n$
- $\text{sgn}(g)$ sign of g on $2n$ points, $\overline{\text{sgn}}(g)$ sign of g on n parts of size 2
- M_{12} is the Mathieu group

Composition tree for a group



Porter-Novelli, Wild Bear, October 2019

1983 Diaconis, Graham and Kantor

“Central symmetry” preserved by in-shuffle and out-shuffle

Starting order: (0,1,2,3,4,5,6,7,8,9,10,11)

After the out-shuffle: (0,6,1,7,2,8,3,9,4,10,5,11)

After the in- shuffle: (6,0,7,1,8,2,9,3,10,4,11,5)

Typical Shuffle group involves: n or $n - 1$ copies of C_2 (one for each pair)

And Symmetric group: $Sym(n)$ permuting these pairs (sometimes only $Alt(n)$)

Typically shuffle group has size: $2^n \times n! > 2^n e^n$

Extraordinary special case: $n = 2^f$ where the group size is only

$$2^n \times (f + 1) \approx 2^n \log n$$

Two small cases: $n = 6, 12$ where the group involves a group smaller than $Sym(n)$, namely $PGL_2(5)$ or M_{12} (a sporadic Mathieu group)

THE UNIVERSITY OF
WESTERN
AUSTRALIA

Dynkin Diagrams of Simple Lie Algebras

A_n

B_n

C_n

D_n

E_6

F_4

G_2

$E_{6,7,8}$

$A_1(4), A_1(5)$	$A_2(2)$											${}^2A_1(4)$	$B_2(3)$	$C_3(3)$	$D_4(2)$	${}^2D_4(2^2)$	$G_2(2)'$	${}^2A_2(9)$
60	168											25 920	4 385 351 680	174 182 400	197 406 720	6 048		
$A_1(9), B_2(2)'$	$A_1(8)$											$B_2(4)$	$C_3(5)$	$D_4(3)$	${}^2D_4(3^2)$	${}^2A_2(16)$		
360	504											979 200	228 501 000 000 000	4 952 179 814 400	10 131 968 619 520	62 400		
A_7	$A_1(11)$	$E_6(2)$	$E_7(2)$	$E_8(2)$	$F_4(2)$	$G_2(3)$	${}^3D_4(2^3)$	${}^2E_6(2^2)$	${}^2B_2(2^3)$	Tits*	${}^2F_4(2)'$	${}^2G_2(3^3)$	$B_3(2)$	$C_4(3)$	$D_5(2)$	${}^2D_5(2^2)$	${}^2A_2(25)$	
2 520	660	214 841 575 522 005 375 270 400	7 995 676 082 479 789 738 480 244 880 952 480	447 881 624 640 479 789 738 480 244 880 952 480	3 311 126 603 566 400	4 245 696	211 341 312	76 332 479 683 774 833 939 200	29 120	17 971 200	10 073 444 472	1 451 520	63 784 736 654 489 600	23 499 295 948 800	25 013 379 358 400	126 000		
$A_3(2)$	A_8	$E_6(3)$	$E_7(3)$	$E_8(3)$	$F_4(3)$	$G_2(4)$	${}^3D_4(3^3)$	${}^2E_6(3^2)$	${}^2B_2(2^5)$	${}^2F_4(2^3)$	${}^2G_2(3^5)$	$B_2(5)$	$C_3(7)$	$D_4(5)$	${}^2D_4(4^2)$	${}^2A_3(9)$		
20 160	1 092	7 200 347 841 683 200 023 295 392 344 632 00	1 271 074 285 176 732 240 479 789 738 480 244 880 952 480	1 271 074 285 176 732 240 479 789 738 480 244 880 952 480	5 734 420 792 816 671 844 761 600	251 596 800	20 560 631 566 912	14 400 000 000 000 000 764 122 480 000 000 000	32 537 600	264 905 352 699 386 176 614 400	49 825 637 439 340 532	4 680 000	273 457 218 604 953 600	8 911 339 000 000 000 000	67 536 471 195 648 000	3 265 920		
A_9	$A_1(17)$	$E_6(4)$	$E_7(4)$	$E_8(4)$	$F_4(4)$	$G_2(5)$	${}^3D_4(4^3)$	${}^2E_6(4^2)$	${}^2B_2(2^7)$	${}^2F_4(2^5)$	${}^2G_2(3^7)$	$B_2(7)$	$C_3(9)$	$D_5(3)$	${}^2D_4(5^2)$	${}^2A_2(64)$		
181 440	2 448	53 502 750 752 342 480 93 883 476 900 140 324 462 346 880 000	53 502 750 752 342 480 93 883 476 900 140 324 462 346 880 000	53 502 750 752 342 480 93 883 476 900 140 324 462 346 880 000	19 009 925 521 840 845 451 297 469 120 000	5 859 000 000	67 862 350 642 790 400	535 676 147 477 000 488 964 172 380 160 964 040 000 000 000	34 093 383 680	1 329 833 323 799 961 487 701 841 409 762 722 540 800	239 189 910 264 3 524 349 332 632	138 297 600	54 025 731 402 499 584 000	1 289 512 799 941 385 139 200	17 880 205 250 600 000 000	5 515 776		
A_n	$A_n(q)$	$E_6(q)$	$E_7(q)$	$E_8(q)$	$F_4(q)$	$G_2(q)$	${}^3D_4(q^3)$	${}^2E_6(q^2)$	${}^2B_2(2^{2n+1})$	${}^2F_4(2^{2n+1})$	${}^2G_2(3^{2n+1})$	$B_n(q)$	$PSp_{2n}(q)$	$O_{2n}^+(q)$	${}^2D_n(q^2)$	$PSU_{n,1}(q)$		
$n \geq 2$	$q^{n(n-1)/2} \prod_{i=1}^{n-1} (q^i - 1)$	$q^{n(n-1)/2} \prod_{i=1}^{n-1} (q^i - 1)$	$q^{n(n-1)/2} \prod_{i=1}^{n-1} (q^i - 1)$	$q^{n(n-1)/2} \prod_{i=1}^{n-1} (q^i - 1)$	q^{n													

Alternates ¹	Symbol	Order ²
-------------------------	--------	--------------------

⁷For sporadic groups and families, alternate names in the upper left are other names by which they may be known. For specific non-sporadic groups these are used to indicate isomorphism. All such isomorphisms appear in the table except the family $A_n(2^m) \cong C_n(2^m)$.

The groups starting on the second row are the classical groups. The sporadic Suzuki group is unrelated to the families of Suzuki groups.

[†]Finite simple groups are determined by their order with the following exceptions:
 $B_2(q)$ and $C_n(q)$ for q odd, $n \geq 2$;
 $A_5 \cong A_3(2)$ and $A_2(4)$ of order 20160.

Copyright © 2012 Ivan Andrus.

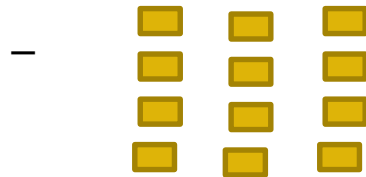
M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	$J(1), J(11)$	HJ	HJM			d_1, HJM, d_{11}	
7 920	95 040	443 520	10 200 960	244 823 040	175 560	604 800	50 232 960	86 755 521 016 077 562 880	44 352 000	898 128 000	4 030 387 200 145 926 144 000

S_z	$O'NS, O-S$	-3	-2	-1	F_{5D}	LyS	F_{5E}	$M(22)$	$M(23)$	$F_{3,1}, M(24)'$	F_2	F_1, M_1
Suz	$O'N$	Co_3	Co_2	Co_1	HN	Ly	Th	Fi_{22}	Fi_{23}	Fi'_{24}	B	M
448 345 497 60	460 813 303 920	493 766 636 000	42 305 421 312 000	4 157 776 806 543 360 000	273 030 912 000 000	51 765 179 004 000 000	97 045 613 887 872 000	4 088 470 473 293 004 800	4 088 470 473 293 004 800	1 255 265 709 190 661 721 292 800	41 520 741 226 400 191 177 000 000 000 000	806027 424 700 302 025 806027 424 700 302 025

“many handed shuffler”

A deck containing kn cards:

- Cut into k piles of n cards each
- “Perfectly interleave them” – What should this mean?
- The **out-shuffle** σ “picks up” top card from each pile in turn, and repeats
 - For $k = 3, n = 4$ the deck $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)$
 - is mapped to $(0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7, 11)$
 - With associated perm: $(0)(1, 3, 9, 5, 4)(2, 6, 7, 10, 8)(11)$



But what should the in-shuffle be?

Rethink the case $k = 2$,

- **In-shuffle same as “swap piles” followed by out-shuffle**

“many handed shuffler”

A deck containing kn cards:

- Cut into k piles of n cards each
- “Perfectly interleave them” – What should this mean?
- Will have the **out-shuffle** σ “picks up” top card from each pile in turn, ...
- Allow an **arbitrary subgroup** $P \leq \text{Sym}(k)$ of the k piles to form the

Generalised shuffle group $G = Sh(P, n) \leq \text{Sym}(kn)$

Not first to study many handed shuffler: 1980's

- Steve Medvedoff and Kent Morrison Math Magazine 1987
- John Cannon – early computational information.

1984 Computations: John Cannon & Kent Morrison

b n	12	24	36	48	60
$n \equiv 0$	A_5 acting on 2 orbits of length 6. $6+6$	$2^{11}.M_{12}$	$2^{17}.A_{18}$	$2^{23}.A_{24}$	$2^{29}.A_{30}$
$n \equiv 1$	$Z_2 \text{ wr } S_4$ $1+6+8$ $\checkmark$ FM	$Z_2 \text{ wr } Z_3$	$(2^8.A_9).(Z_2 \text{ wr } S_{10})$ $1+18+20$ $e \quad o$ odd	$(2.M_{12}).(Z_2 \text{ wr } A_{13})$ $1+24+26$ $e \quad o$ odd	$(2^{14}.A_{15}).(Z_2 \text{ wr } S_{16})$ $1+30+32$ $e \quad o$ odd
$n \equiv 2$	$Z_2 \text{ wr } S_9$ 18 $\checkmark$	$Z_2 \text{ wr } S_{15}$ 30 $\checkmark$	$Z_2 \text{ wr } S_{21}$ 42 $\checkmark$	$Z_2 \text{ wr } S_{27}$ 54 $\checkmark$	$Z_2 \text{ wr } S_{33}$ 66 $\checkmark$
$n \equiv 3$	$(2^4.A_5).(2^4.D_5)$ $(2^4.Z_5).(2^4.S_5)$ $1+10+10$ odd even $\checkmark$	$(2^7.A_8).(Z_2 \text{ wr } S_8)$ $1+16+16$ even $\checkmark$	$(2^{10}.L_2(11)).(2^{10}.S_{11})$ $1+22+22$ even $\checkmark$	$(2^{13}.A_{14}).(Z_2 \text{ wr } S_{14})$ $1+28+28$ even $\checkmark$	$(2^{16}.A_{17}).(2^{16}.S_{17})$ $1+34+34$ even $\checkmark$

Focused on the case of $G = Sh(Sym(k), n)$ that is $P = Sym(k)$

1. $kn = k^f$ (“power case”) turned out to give “exceptionally small” G

$$\text{If } kn = k^f \text{ then } Sh(Sym(k), k^{f-1}) = Sym(k)^f \cdot C_f$$

2. Worked out precisely when $Sh(Sym(k), n) \subseteq Alt(kn)$ contains only even permutations [in terms of $n, k \pmod{4}$]

3. Explored cases $k=3$ and $k=4$ computationally for small n and

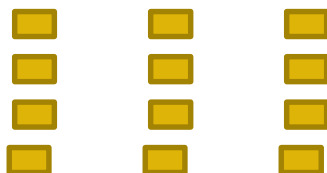
4. **MM Conjecture:** if $kn \neq k^f$ and $kn \neq 4 \cdot 2^f$ then $Sh(Sym(k), n)$ should be $Sym(kn)$ or $Alt(kn)$

Explored $G = Sh(P, n)$ for general $P \leq Sym(k)$

- Show the “power case” where $kn = k^f$ is also special for general P
- Show certain properties of P lead to similar properties of G
- Confirm the MM-Conjecture [that G usually contains $Alt(kn)$] in 3 cases:
 - $k > n$
 - $k = 2^e \geq 4$
 - $k = \ell^e$ and $n = \ell^f$ for some ℓ, e and f
- We gained insights leading to new open questions

Suppose $P \leq \text{Sym}(k)$ is transitive. Is $G = \text{Sh}(P, n)$ transitive?

- The answer is “yes” – transitive P gives transitive G
- To see this use $\rho: P \rightarrow G$ where for $\tau \in \text{Sym}(k)$, $\rho(\tau)$ means “permute the piles according to τ ”



In Example $k = 3, n = 4$

For $\tau = (0,1) \in \text{Sym}(3)$,
 $\rho(\tau) = (0,4)(1,5)(2,6)(3,7)$

Label Deck as $[kn] = \{0, 1, \dots, kn - 1\}$

So set of piles is $[k] = \{0, 1, \dots, k - 1\}$

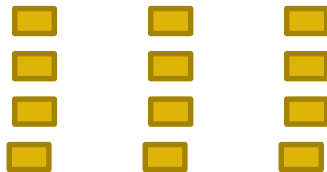
Pile 0 has cards $\{0, 1, \dots, n - 1\}$

Suppose $P \leq \text{Sym}(k)$ is transitive. Is $G = \text{Sh}(P, n)$ transitive?

$\rho(P)$ has the horizontal layers as its “orbits”

- We examine the shuffle σ and check that it “merges” all these orbits
- The shuffle maps $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)$
- To $(0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7, 11)$

In Example
 $k = 3, n = 4$

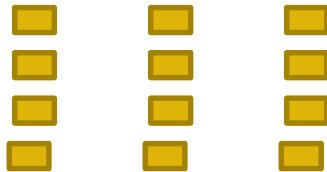


So the shuffle σ is
 $(0)(1, 3, 9, 5, 4)(2, 6, 7, 10, 8)(11)$

So $1 \rightarrow 3.1$, $2 \rightarrow 3.2$, $3 \rightarrow 3.3$, $4 \rightarrow 1 = 3.4 - 11$, $5 \rightarrow 4 = 3.5 - 11$,
 $6 \rightarrow 7 = 3.6 - 11$, $7 \rightarrow 10 = 3.7 - 11$, $8 \rightarrow 2 = 3.8 - 22$, ...

Suppose $P \leq \text{Sym}(k)$ is transitive. Is $G = \text{Sh}(P, n)$ transitive?

- We examine the shuffle σ and check that it “merges” all these orbits



Each intransitive subgroup P of $\text{Sym}(3)$ gives an intransitive shuffle group $G = \text{Sh}(P, 4)$ - but general case not settled

Shuffle:

σ fixes 0 and otherwise maps card

a

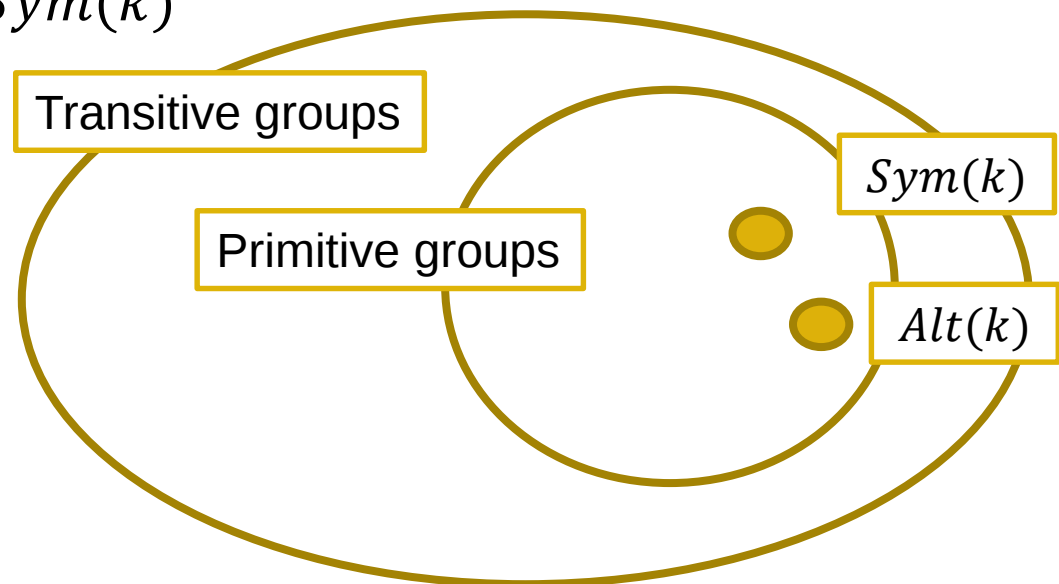
To card

$ka \pmod{kn - 1}$

The remainder between 1 and $kn - 1$ after dividing ka by $kn - 1$

What other properties are interesting?

Transitive subgroups of $Sym(k)$



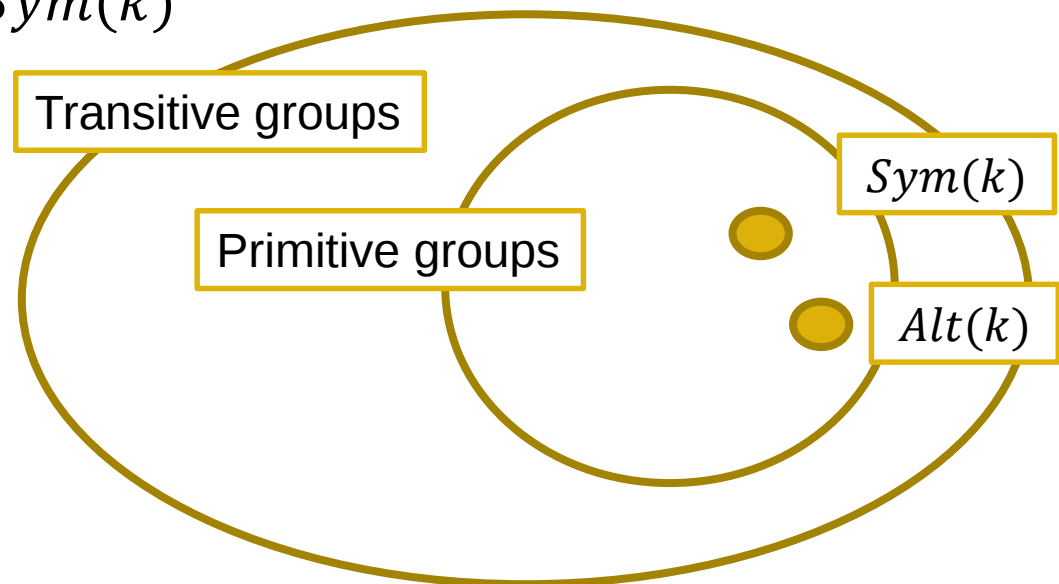
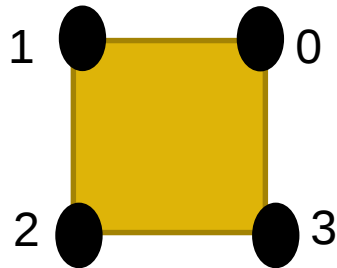
Primitive: “only invariant partitions are trivial”

Good tools for studying primitive groups

What other properties are interesting?

Transitive subgroups of $Sym(k)$

$\{0, 2 \mid 1, 3\}$ invariant for
 $P = \langle (0123), (13) \rangle \leq Sym(4)$



Primitive: “only invariant partitions are trivial”

Good tools for studying primitive groups

Primitive groups: regular or not?

Regular permutation group $P \leq \text{Sym}(k)$: for each point pair (α, β) exactly one $g \in P$ maps $\alpha \rightarrow \beta$

Fact: If $P \leq \text{Sym}(k)$ and P is **primitive and regular**, then $k = p$ is prime and $P \cong C_p$ is cyclic of order p

- Recall: if $k = 2$ then $P = \text{Sym}(2) \cong C_2$ and $G = \text{Sh}(\text{Sym}(2), n)$ is not primitive [“central symmetry” preserved]

Theorem: If $P \leq \text{Sym}(k)$ is primitive and **not** regular then $G = \text{Sh}(P, n)$ **primitive**

Primitive groups: regular or not?

Regular permutation group $G \leq \text{Sym}(k)$: for each point pair $\{\alpha, \beta\}$ exactly one $g \in G$ maps $\alpha \rightarrow \beta$

Fact: If $G \leq \text{Sym}(k)$ and G is primitive and regular, then $k = p$ is prime and $G \cong C_p$ is cyclic of order p

- Recall: if $k = 2$ then $P = \text{Sym}(2) \cong C_2$ and $G = \text{Sh}(\text{Sym}(2), n)$ is not primitive [“central symmetry” preserved]
- If $k = p$ is odd then $G = \text{Sh}(C_p, n)$ is imprimitive if $n = p^f$

is $\text{Alt}(kn)$ or $\text{Sym}(kn)$ if $n \neq p^f$ IF $p \leq 13, n \leq 1000$
AND WE CONJECTURE THIS TRUE FOR ALL $n \neq p^f$

Theorem: If $P \leq \text{Sym}(k)$ is primitive and not regular then $G = \text{Sh}(P, n)$ primitive

1. The Power case: $n = k^f$, and any $P \leq \text{Sym}(k)$ implies that $G = \text{Sh}(P, n) = P \wr C_{1+f}$ [i.e. SMALL]

[generalises DGK and MM]

2. Other interesting structure preservation happens:

AFFINE STRUCTURE:

$[k]$ = finite vector space and each $x \in P$ acts as a nonsingular linear transformation followed by a translation

- If P preserves an “affine structure” on $[k] = F_p^e$ then $G = \text{Sh}(P, n)$ preserves an affine structure on $[kn]$ “whenever it can”
 - If $n = p^f$ then $G = \text{Sh}(P, n)$ preserves affine structure on $[kn] = F_p^{e+f}$
 - If $n \neq p^f$ and if $k > n$, and if P is 2-transitive, then $G = \text{Sh}(P, n)$ is $\text{Alt}(kn)$ of $\text{Sym}(kn)$ [proves MM conjecture for this situation: relies on FSGC]

1. The Power case: $n = k^f$, and any $P \leq \text{Sym}(k)$ implies that $G = \text{Sh}(P, n) = P \wr C_{1+f}$ [i.e. SMALL]

[generalises DGK and MM]

2. Other interesting structure preservation happens:

PRODUCT STRUCTURE:

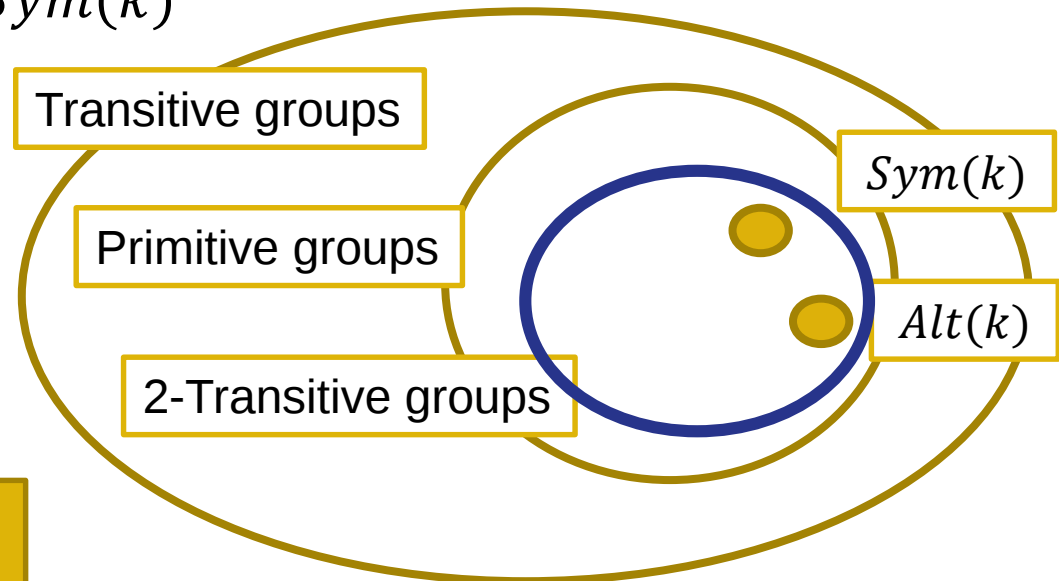
$[k] = \ell \times \cdots \times \ell = [\ell]^e$ and each $x \in P$ acts independently on each entry of a point $(\alpha_1, \dots, \alpha_e)$ with elements of $\text{Sym}(\ell)$ followed by a permutation of the entries

If P preserves a “product structure” on $[k] = [\ell]^e$ then $G = \text{Sh}(P, n)$ preserves a product structure on $[kn] = [\ell]^{e+f}$

“whenever it can”, that is, whenever $[n] = [\ell]^f$

Amarra, Morgan and CEP: what else, $k \geq 3$?

Transitive subgroups of $Sym(k)$



Focus: $P = Sym(k)$
So in particular P is 2-transitive

2-Transitive: $P \leq Sym(k)$ transitive and stabiliser P_0
transitive on $[k] \setminus \{0\}$

Amarra, Morgan and CEP: what else, $k \geq 3$?

We show: if $k > n > 2$ and $P \leq \text{Sym}(k)$ is 2-transitive then $G = \text{Sh}(P, n)$ is 2-transitive.

We asked ourselves: Since finite 2-transitive groups are known explicitly (using the finite simple group classification) Can we be more specific?

Fact: P is 2-transitive implies P is “almost simple” or affine

1. Affine case: we already discussed
2. Almost simple case: we prove $\text{Sh}(P, n)$ is almost simple
3. Moreover: if P is $\text{Alt}(k)$ or $\text{Sym}(k)$ then $\text{Sh}(P, n)$ is $\text{Alt}(kn)$ or $\text{Sym}(kn)$

[proving MM conjecture in this case]

Cascading shuffle groups

One last investigation, then summary and questions:

Suppose $k = 2^e \geq 4$ and $n \neq 2$ -power.

For $t \in \{1, 2, \dots, e\}$, the deck $[kn] = [2^t \cdot 2^{e-t}n]$ and $G_t = Sh(\textcolor{red}{C}_2^t, 2^{e-t}n)$ all groups transitive on $[kn]$

How are they related? Note that G_1 is known from [DGK]

With much hard work and misgivings we proved that

$$G_1 \geq G_2 \geq \dots \geq G_e$$

Generically: all the G_t equal and all preserve central symmetry

Theorem If $k = 2^e \geq 4$ and $n \neq 2$ -power, then $Sh(\textcolor{red}{Sym}(k), n)$ is $Alt(kn)$ or $Sym(kn)$

Summary and questions for $k \geq 3$

MM Conjecture Still Open: if $kn \neq k^f$ and $kn \neq 4 \cdot 2^f$ then $Sh(Sym(k), n)$ should be $Alt(kn)$ or $Sym(kn)$

Our contribution: we have confirmed it for:

- $k > n$
- $k = 2^e$
- $k = \ell^e$ and $n = \ell^f$ for some ℓ, e, f

Work led to our own conjectures: first

If k is an odd prime, $k < n$, and n is not a power of k , then $Sh(C_k, n)$ should be $Alt(kn)$ or $Sym(kn)$

More questions

Diaconis is particularly interested in $P = \langle \tau \rangle$ where τ “reverses the piles”

Not much in [MM] or our paper [AMP]

But recent computational evidence suggests some very interesting groups arise. Perhaps at last we’ll be able to make sense of the computational data from John Cannon and Kent Morrison’s data

More questions

Diaconis is particularly interested in $P = \langle \tau \rangle$ where τ “reverses the piles”

Not much in [MM] or our paper [AMP]

But recent computational evidence suggests some very interesting groups arise. Perhaps at last we’ll be able to make sense of the computational data from John Cannon and Kent Morrison’s data

Thank you

