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

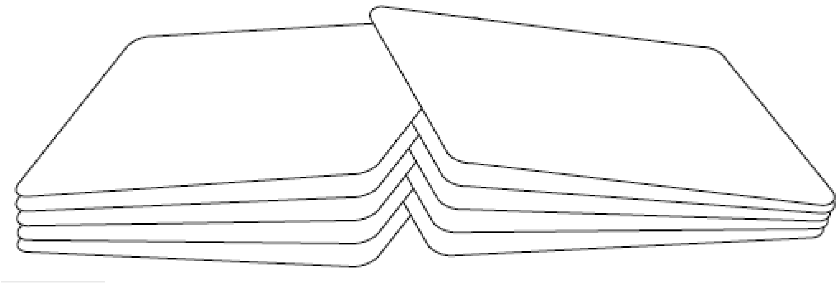
Starting order: (0,1,2,3,4,5,6,7,8,9,10,11)
After the in– shuffle: (6,0,7,1,8,2,9,3,10,4,11,5)

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 $o(2, mod\ 2n-1)$
- Golomb 1961, deck of 2n-1 cards: Group order is $(2\mathrm{n}-1)\times o(2, mod\ 2n-1)$
- 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 $\sigma = O$ and $\delta =$ swap the piles, so $I = \delta \circ \sigma$ and shuffle group is $\langle \sigma, \delta \rangle$,

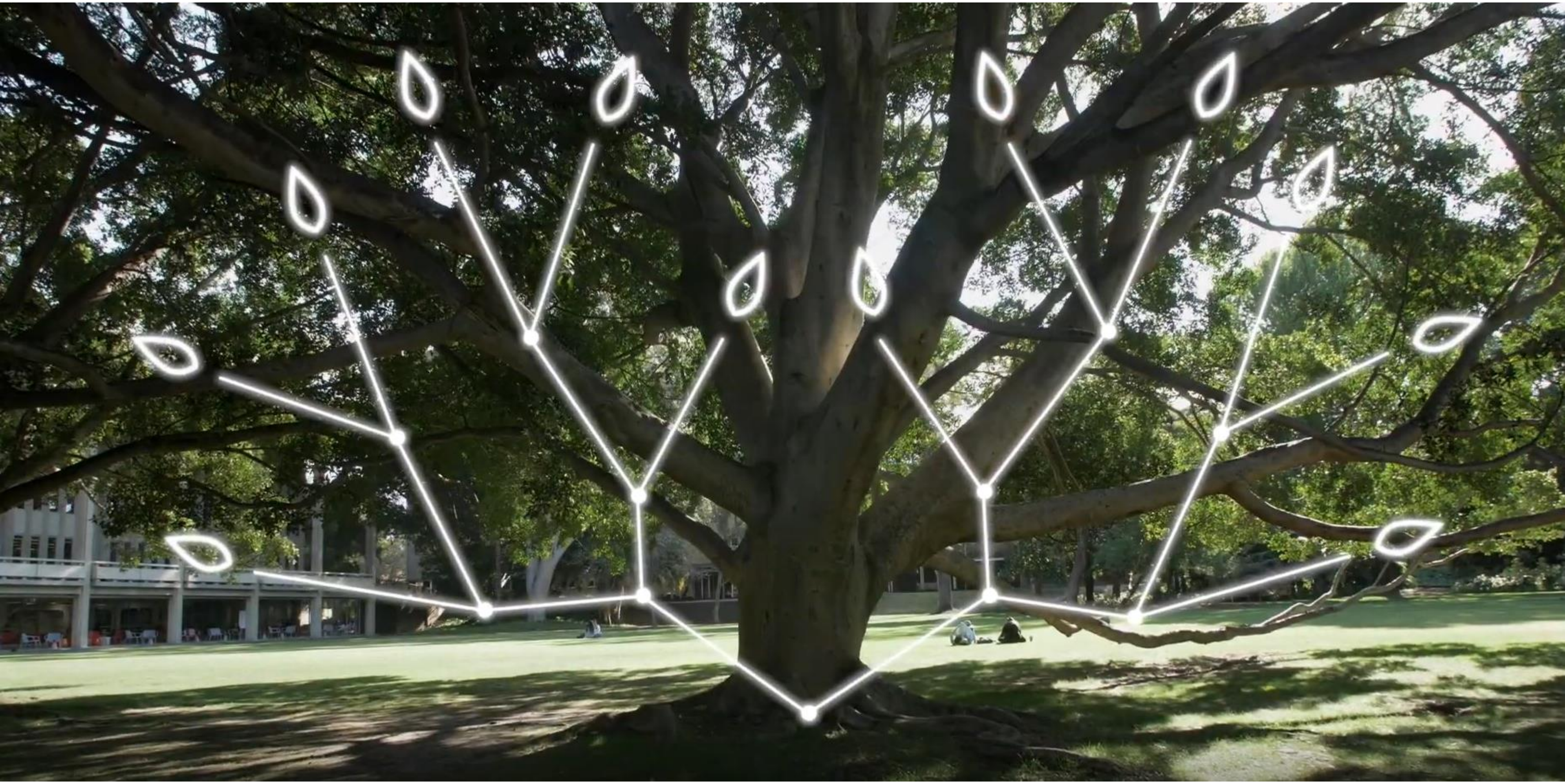
Theorem 1.1. [8, Theorem 1] *The structure of the shuffle group $\langle \sigma, \delta \rangle$ on $2n$ points, where $n \geqslant 2$, is given in Table 1.*

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

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

- $B_n = C_2 \wr Sym(n) \leq Sym(2n)$, for $g \in B_n$
- $sgn(g)$ sign of g on 2n points, $\overline{sgn(g)}$ 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 $Alt(n)$)

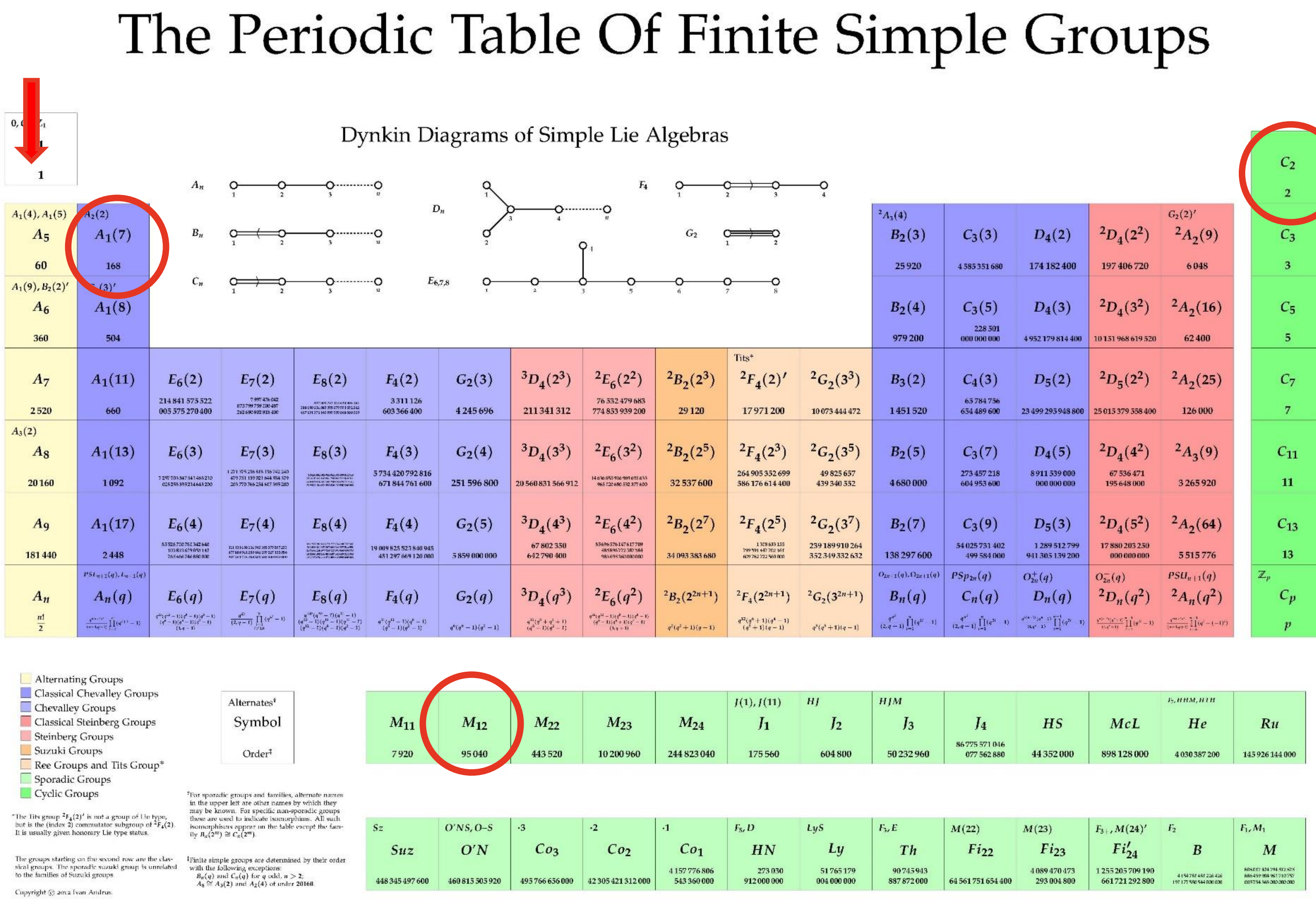
Typically shuffle group has size: $2^n \times n! \;>\; 2^n\, e^n$

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)

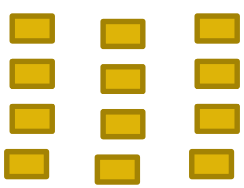
Finite simple group classification



“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** $P \leq Sym(k)$ of the k piles to form the

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

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

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

Medvedoff and Morrison 1987

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

1. $\boldsymbol{kn = k^f}$ **("power case") turned out to give "exceptionally small" G**

   If $kn = k^f$ then $Sh\left(Sym(k), k^{f-1}\right) = Sym(k)^f . C_f$

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

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

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

Amarra, Morgan and CEP

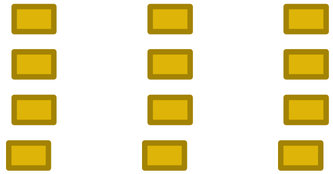
Explored $G = Sh(P, n)$ for general $P \leq Sym(k)$

- 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

Amarra, Morgan and CEP

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

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



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

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

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

In Example $k = 3, n = 4$

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

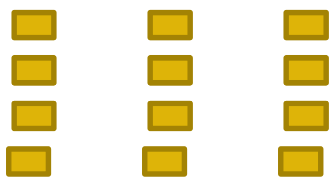
Amarra, Morgan and CEP

Suppose $P \leq Sym(k)$ is transitive. Is $G = Sh(P, n)$ 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
$k = 3, n = 4$



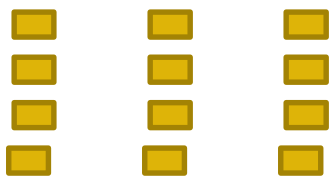
So the shuffle σ is
(0)(1, 3, 9, 5, 4)(2, 6, 7, 10, 8)(11)

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

Amarra, Morgan and CEP

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

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



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

Shuffle:
σ fixes 0 and otherwise maps card

$$a$$

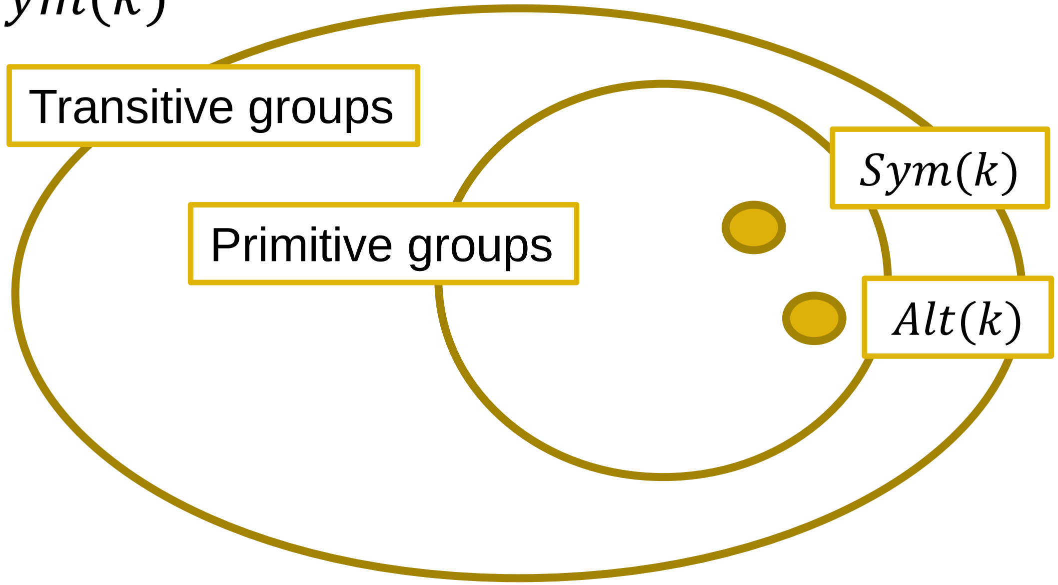
To card

$$ka \ (mod\ kn - 1)$$

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

What other properties are interesting?

Transitive subgroups of $Sym(k)$



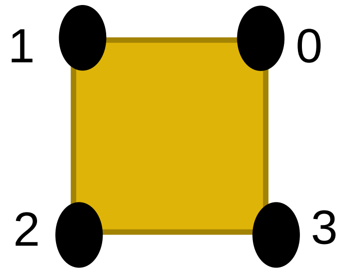
Primitive: “only invariant partitions are trivial”

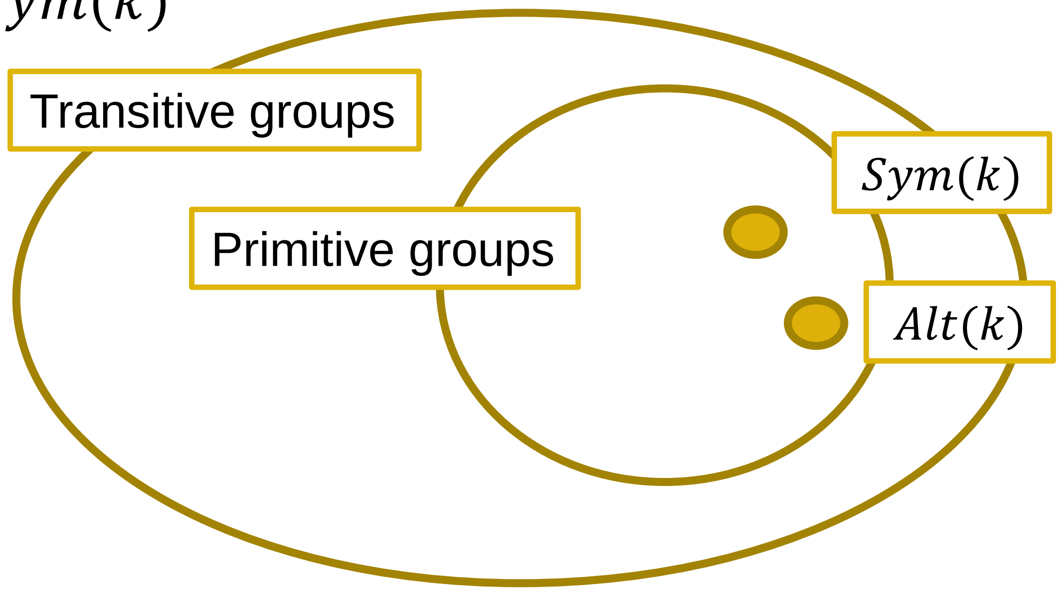
Good tools for studying primitive groups

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

Fact: If $P \leq Sym(k)$ 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 $P = Sym(2) \cong C_2$ and $G = Sh(Sym(2), n)$ is not primitive [“central symmetry” preserved]

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

Primitive groups: regular or not?

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

Fact: If $G \leq Sym(k)$ 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 $P = Sym(2) \cong C_2$ and $G = Sh(Sym(2), n)$ is not primitive ["central symmetry" preserved]
- If $k = p$ is odd then $G = Sh(C_p, n)$ is imprimitive if $n = p^f$

$is\ Alt(kn)$ or $Sym(kn)$ 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 $P \leq Sym(k)$ is primitive and not regular then $G = Sh(P, n)$ primitive

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

1. The Power case: $n = k^f$, and any $P \leq Sym(k)$ implies that $G = Sh(P,n) = P \wr C_{1+f}$ [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 $G = Sh(P,n)$ preserves an affine structure on $[kn]$ "whenever it can"
  - If $n = p^f$ then $G = Sh(P,n)$ 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 $G = Sh(P,n)$ is $Alt(kn)$ of $Sym(kn)$ [proves MM conjecture for this situation: relies on FSGC]

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

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

   [generalises DGK and MM]

2. Other interesting structure preservation happens:

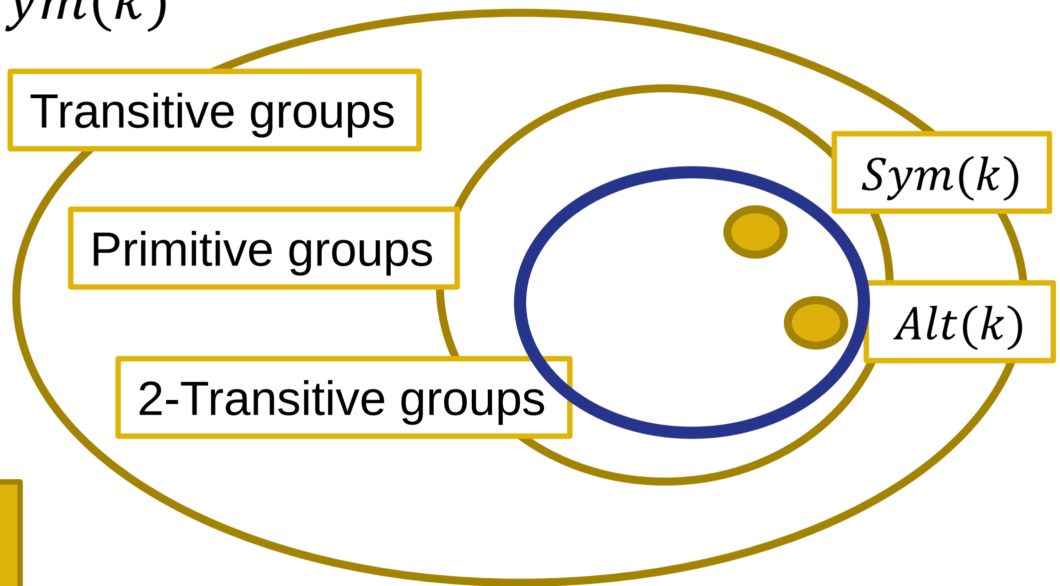
PRODUCT STRUCTURE:

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

If P preserves a "product structure" on $[k] = [\ell]^e$ then $G = Sh(P, n)$ 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, $k \geq 3$?

THE UNIVERSITY OF WESTERN AUSTRALIA

We show: if $\boxed{k > n > 2}$ and $P \leq Sym(k)$ is 2-transitive then $G = Sh(P, n)$ 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 $Sh(P, n)$ is almost simple
3. Moreover: if P is $Alt(k)$ or $Sym(k)$ then $Sh(P, n)$ is $Alt(kn)$ or $Sym(kn)$

[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 $t \in \{1,2,\ldots,e\}$, the deck $[kn] = [2^t \cdot 2^{e-t}n]$ and $G_t = Sh(C_2^t, 2^{e-t}n)$ 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

$$G_1 \geq G_2 \geq \cdots \geq G_e$$

Generically: all the G_t equal and all preserve central symmetry

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

Summary and questions for $k \geq 3$

THE UNIVERSITY OF WESTERN AUSTRALIA

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 $Sh(\boldsymbol{C_k}, n)$ 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