Shuffle Groups

Joint work with Carmen Amarra and Luke Morgan

Cheryl E Praeger

Centre for the Mathematics of Symmetry and Computation

Groups and Geometries

Banff, Aug 2019

Perfect Shuffles

THE UNIVERSITY OF WESTERN AUSTRALIA

A deck containing 2n cards:

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

Out – shuffles and in - shuffles

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

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

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

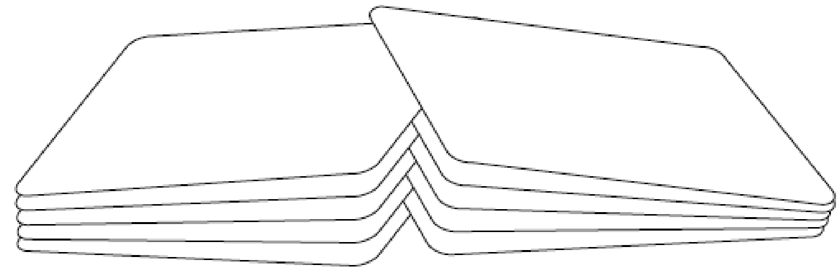
Questions (from card-players):

- how many times to regain original order?
- Can I get card 0 into any chosen position by repeated out or in shuffles?

What is a shuffle group?

A deck containing 2n cards:

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



Out – shuffles and in - shuffles

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

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

- O = (0)(1,2,4,8,5,10,9,7,3,6) (11)

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

- I = (0,1,3,7,2,5,11,10 ,8,4,9,6)

Shuffle group is the subgroup of Sym(2n) generated by O and I.

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 (2n-1) x 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

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

“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 $k = 3, n = 2$ the deck $(0,1,2,3,4,5)$ is mapped to $(0,3,5,1,4,6)$
- Allow an **arbitrary subgroup** $P \leq Sym(k)$ of the k piles to form the

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

Not first to study this: 1980’s

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

1984 Computations: John Cannon & Kent Morrison

n \ 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 wr S_4 ✓KM.	Z_2 wr Z_3	1+18+20 (e o) $(2^8.A_9).(Z_2$ wr $S_{10})$ odd	1+24+26 (e o) $(2.M_{12}).(Z_2$ wr $A_{13})$ odd ✓	1+30+32 (e o) $(2^{14}.A_{15}).(Z_2$ wr $S_{16})$ odd ✓
$n \equiv 2$	18 Z_2 wr S_9 ✓	30 Z_2 wr S_{15} ✓	42 Z_2 wr S_{21}	54 Z_2 wr S_{27} ✓	66 Z_2 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 $(2^7.A_8).(Z_2$ wr $S_8)$ even ✓	1+22+22 $(2^{10}.L_2(11)).(2^{10}.S_{11})$ even ✓	1+28+28 $(2^{13}.A_{14}).(Z_2$ wr $S_{14})$ even ✓	1+34+34 $(2^{16}.A_{17}).(2^{16}.S_{17})$ even ✓

Medvedov and Morrison 1987

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

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

We write the deck as $[kn] = \{0,1,\ldots,kn-1\}$

- If $kn = k^f$ then $Sh\left(Sym(k), k^{f-1}\right) = Sym(k) \wr C_f$ in product action on $[k]^f$

Showed that $Sh(Sym(k), n) \subseteq Alt(kn)$ if and only if

- either $n \equiv 0\ (mod\ 4)$ or $(k\ mod\ 4, n\ mod\ 4)$ is (0,2) or (1,2)

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

Conjectured that 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

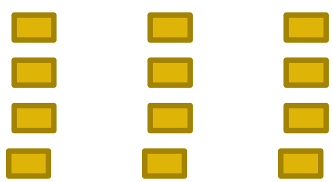
Explored $G = Sh(P, n)$ for general $P \leq Sym(k)$

- 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:
  - $k > n$
  - $k = 2^e \geq 4$ and $n \neq 2^f$ for any f
  - $k = \ell^e \neq 4$ and $n = \ell^f$ for some ℓ where e does not divide f
- We are left with several open questions

Amarra, Morgan and CEP

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

- The answer is "yes" but the converse does not hold.
- 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 $[kn] = \{\, 0,1, \dots, kn - 1\}$

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

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

In Example $k = 3, n = 4$

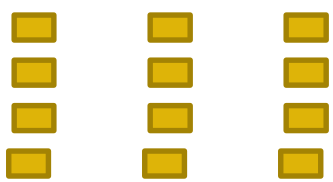
For $\tau = (0,1) \in Sym(3)$,
$\rho(\tau) = (0,4)(1,5)(2,6)(3,7)$

Amarra, Morgan and CEP

THE UNIVERSITY OF WESTERN AUSTRALIA

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

- If P is transitive then $\rho(P)$ has as orbits the rows: $\{ 0, n, \dots, (k-1)n\}, etc$
- We examine the `shuffle' σ and check that it "merges" all these orbits



Deck starts as
$(0,1,2, 3, 4, \dots, 11)$
σ maps this order to
$(0,4,8,1, 5 \dots, 11)$
So cards 1, 2 in row 0 are mapped to cards in row 1, 2;
And card 3 in row 3 is mapped to 1 in row 1.

But many intransitive subgroups P still have transitive shuffle groups $G = Sh(P, n)$

Amarra, Morgan and CEP

1. Suppose $P \leq Sym(k)$ is primitive but not C_p acting regularly. Then $G = Sh(P, n)$ primitive.
   - So $Sh(Sym(k), n)$ primitive if and only if $k \geq 3$
   - [so DGK case $k = 2$ is exceptional in this respect]

2. The Power case: $n = k^f$, and any $P \leq Sym(k)$ implies that $G = P \wr C_{1+f}$ [generalises DGK and MM]
3. Other interesting structure preservation happens:
   - Suppose that $k = \ell^e$, $n = \ell^f$, e does not divide f then
   - When $P = Sym(\ell) \wr Sym(e)$ in product action on $[\ell]^e$ then $G = Sym(\ell) \wr Sym(e+f)$ in product action on $[\ell]^{e+f}$
   - When $P = AGL(e, \ell)$ and ℓ is prime then $G = AGL(e+f, \ell)$
   - When $k \neq 4$, then $Sh(Sym(k), n)$ contains $Alt(k\ n)$ [proving MM conjecture for these parameters]

Amarra, Morgan and CEP

1. Suppose $P \leq Sym(k)$ is primitive but not $C_p$acting regularly. Then $G = Sh(P, n)$ primitive.
   – So $Sh(Sym(k), n)$ primitive if and only if $k \geq 3$
   – [so DGK case $k = 2$ is exceptional in this respect]

2. Computationally if $k \leq 13$ and $k < n \leq 1000$, and n is not a power of k, then $Sh(C_k, n)$ contains $Alt(kn)$

We Conjecture: If k is an odd prime, n > k, and n is not a power of k, then $Sh(C_k, n)$ contains $Alt(kn)$

Amarra, Morgan and CEP

Suppose that k > n > 2 and that $P \leq Sym(k)$ is 2-transitive
Then $G = Sh(P, n)$ is 2-transitive.

We asked ourselves: Since finite 2-transitive groups are known can we be more specific?

First for P almost simple 2-transitive, and k > n > 2

a. Then also $Sh(P, n)$ is almost simple;
b. And if P is Alt(k) or Sym(k) then $Sh(P, n)$ contains Alt(kn) or $kn = 4 \cdot 2 = 8$ and $Sh(P, n) = AGL(3,2)$

Amarra, Morgan and CEP

Now for P affine 2-transitive, and $k = p^e > n > 2$

(1) No chance of Sh(P,n) affine unless $n = p^f$

- $n = p^f$ case covered in the “power case”:
- $Sh(P, n) \leq Sh(AGL(e, p), n) = AGL(e + f, p)$

(2) Outstanding case: $n \neq p^f$

- Clearly $Sh(P, n)$ not affine as $kn \neq p^a$
- Maybe $Sh(P, n)$ should be $Alt(kn)$ or $Sym(n)$

We proved this using the classification of 2-transitive groups
+++

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

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

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

Summary and questions

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

Our contribution to confirm it for:

- $k > n$
- $k = 2^e \geq 4$ and $n \neq 2^f$ for any f
- $k = \ell^e \neq 4$ and $n = \ell^f$ for some ℓ where e does not divide f

Our first Conjecture: If k is an odd prime, n > k, and n is not a power of k, then $Sh(C_k, n)$ contains $Alt(kn)$

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