Group Theory, Card Shuffling and Magic

By Jonathan Tsai

What is a card shuffle?

- Suppose that we have a standard deck of 52 cards.
- A card shuffle mixes the order of the cards:

  e.g. 1^{st} card $\rightarrow$ 32^{nd} card

  2^{nd} card $\rightarrow$ 28^{th} card

  etc.

- Mathematically, we can view a shuffle as a function:

  S: {1,2,...,52} → {1,2,...,52}

  e.g.

  S(1)=32, S(2)=28,...

  This means that the shuffle S takes

  1^{st} card → 32^{nd} card

  2^{nd} card → 28^{th} card

  etc.

- In mathematics, we call a shuffle a **permutation**.
- Note that if S and T are two shuffles, then the **composition**, $T \circ S$, is the shuffle that is obtained by first performing the shuffle S and then performing the shuffle T.

  (Note the order!)

  In other words, $T \circ S(k) = T(S(k))$ for $k=1,2,\ldots 52$

- Let $\mathbf{S}_{52}$ be the set of all shuffles of a 52 card deck.

- The simplest shuffle is the **identity shuffle**, i. It is the “shuffle” that doesn't change the order of the cards i.e.

  $i(1)=1, i(2)=2, \ldots , i(52)=52$

- For any shuffle S, we can find a shuffle T which takes the deck back to its original position. In other words,

  $T \circ S(k)=k$ for $k=1,2,...52$ or $T \circ S=i$

  Note that $T \circ S=i$ implies that $S \circ T=i$

  T is called the **inverse shuffle** of S.

Hence the set of all shuffles, $\mathbf{S}_{52}$, satisfies the following properties:

- (Closure) For any shuffles S and T (in $\mathbf{S}_{52}$), S◦T is also a shuffle.

  (Identity) There is a shuffle, i, such that for any shuffle S,

  S◦i = i◦S = S
- (Inverse) For any shuffle, S, there is a shuffle T such that

  S◦T = S◦T = i
- (Associativity) For any shuffles S, T and U, we have

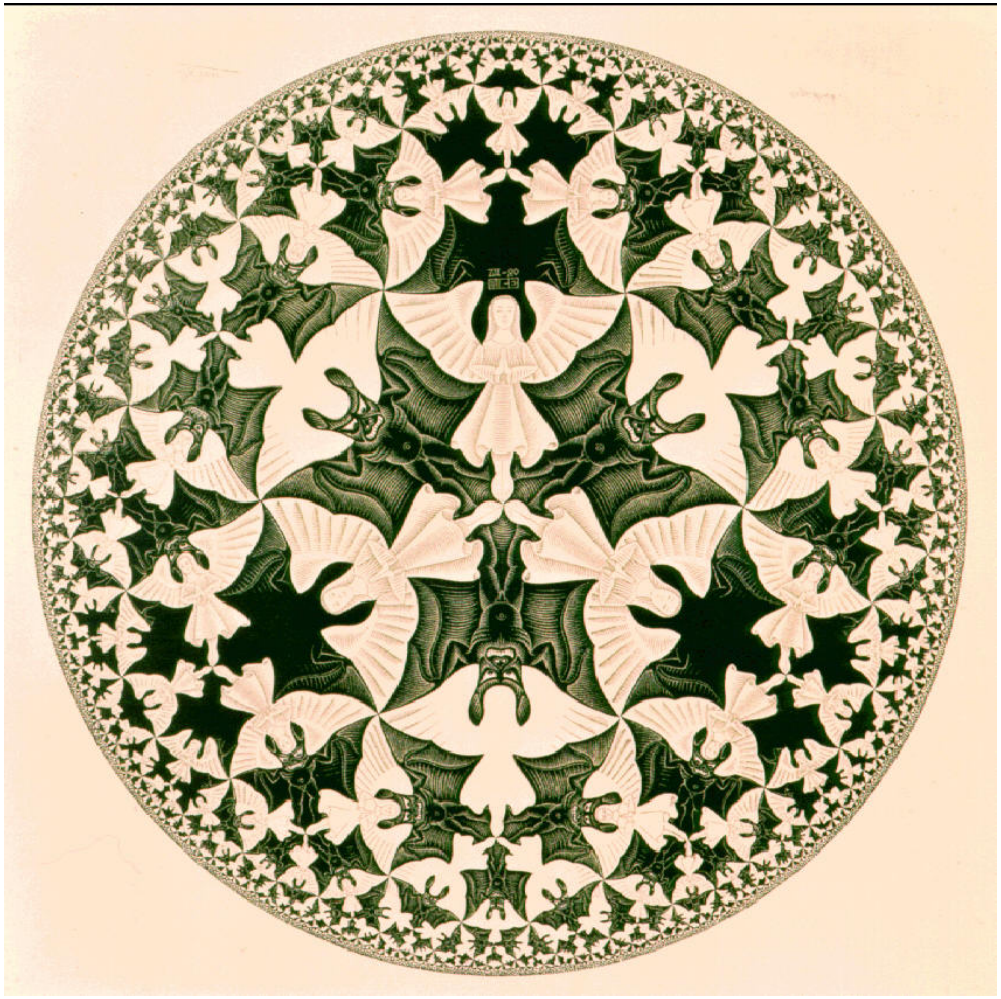
  S◦(T◦U)=(S◦T)◦U

- These properties imply that the set of shuffles $\mathbf{S}_{52}$ with the composition operator $\circ$ form a **group**.
- A group is a set G with some operator $\bullet$ that satisfies the four properties we had previously.
- Groups are immensely important in mathematics. The basic theory was invented by Evariste Galois in order to show that there is no formula to solve quintic (or higher order) equations.

- Groups occur in many different contexts:

  e.g.

  - $\mathbf{Z}_p$ (integers modulo p) is a group with the operator "× mod p" only when p is prime.
  - The set of all Mobius transformations $\mathcal{M}$ with the composition operator is a group. Of particular interest are certain subsets of $\mathcal{M}$ are also groups called **discrete groups**.



Circle Limit IV by
M.C. Escher

- The “symmetries” of this picture correspond to a discrete group of Mobius transformations.

- Certain groups called Lie groups are very important in differential geometry. Lie groups are basically groups that are have “differential structure” (i.e. we can do calculus on them)

Back to Shuffle groups:

- So $\mathbf{S}_{52}$ is a group. Similarly, we can define $\mathbf{S}_N$ to be the set of all shuffles of a deck of N cards. It is clear that $\mathbf{S}_N$ is also a group with the operator $\circ$.
- The main subject of this talk is a special shuffle…

- The main “trick” is the special shuffle that I used which is called the **Perfect shuffle** or **Faro shuffle**.

The Perfect Shuffle

- It is more convenient to label the cards 0,...,N-1
- (i.e. the 1st card is 0, ... , the Nth card is N-1)
- There are 2 types of perfect shuffles.
- The **out (perfect) shuffle**, O_N, is the following:

  e.g. N=10, O_9

  0,1,2,3,4,5,6,7,8,9 → 0,5,1,6,2,7,3,8,4,9

In general, if N is odd

$O_N(k)=2k \bmod N$;

(i.e. the remainder when we divide 2k by N)

if N is even,

$O_N(k)=2k \bmod (N-1)$ for $k=1,\ldots, N-2$

and $O_N(N-1)=N-1$.

e.g. $N=52$, $O_N(33)=15$

- The **in (perfect) shuffle**, I_N, is the following:

  e.g. N=10, I_9

  0,1,2,3,4,5,6,7,8,9 → 5,0,6,1,7,2,8,3,9,4

  In general, if N is odd

  $I_N(k)=2k+1 \bmod N$;

  if N is even

  $I_N(k)=2k+1 \bmod (N+1)$.

- In magic circles, the perfect shuffle is often called the **faro shuffle**.

- One of the keys to the trick “Unshuffled” is the following fact:

  $O_{52} \circ O_{52} \circ O_{52} \circ O_{52} \circ O_{52} \circ O_{52} \circ O_{52} \circ O_{52} = i$

  i.e. Performing 8 out shuffles in a deck of 52 cards is the same as performing the identity shuffle. In other words, 8 out perfect shuffles returns the deck to its original configuration!!!

- To prepare for the trick, I take an unshuffled deck of cards and perform 5 out shuffles to it. 3 more out shuffles then returns the deck to the unshuffled state!

- Using the terminology from group theory, we define the **order** of a shuffle g in S_N to be the smallest p such that

  $f^p = f \circ f \circ \ldots \circ f = I$
- We write order(f)=p
- Hence,

  $order(O_{52})=8$
- Why is this such a small number?
- How can we calculate the order of O_N and I_N?

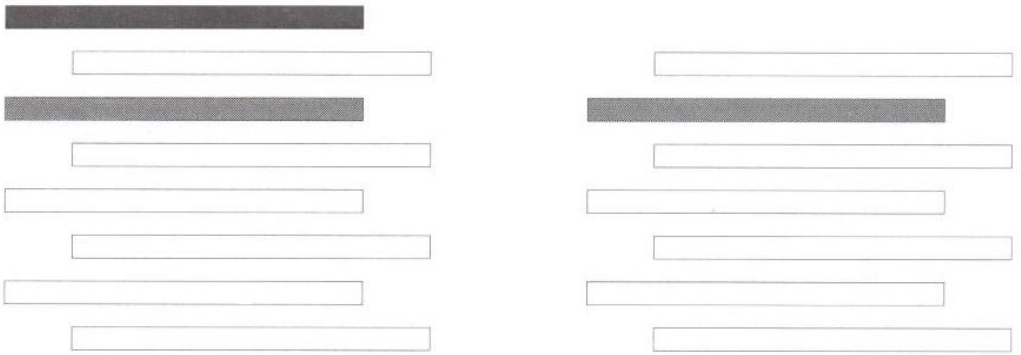
Theorem

- order(O_{2n})=order(O_{2n-1})=order(I_{2n-1})=order(I_{2n-2}) and order(O_{2n})=r,

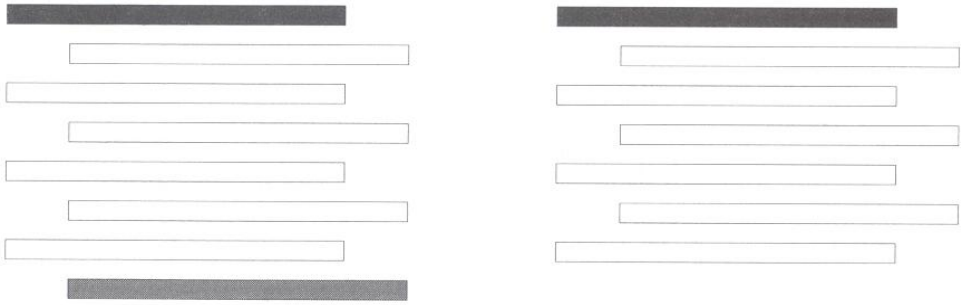
  where r is the smallest number such that $2^r = 1 \bmod (2n-1)$.

Proof:

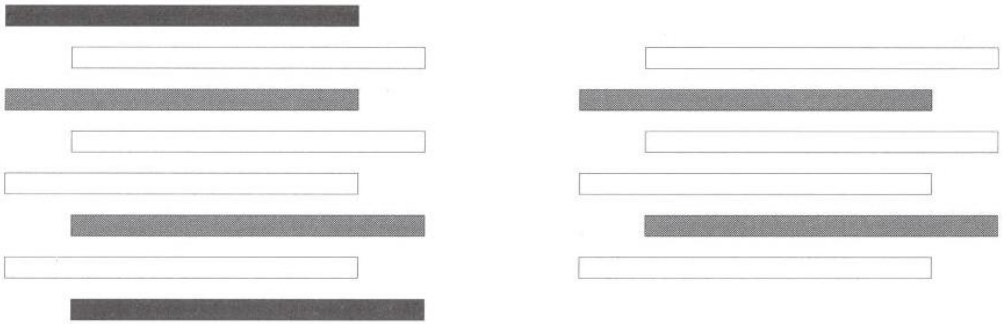
- The following diagrams show that:



- order(O_{2n})=order(O_{2n-1})



- order(O_{2n})=order(I_{2n-1})



- order(O_{2n})=order(I_{2n-2}).

- Recall that in a deck of N=2n cards,

  $O_{2n}(k)=2k \bmod (2n-1)$.

- Hence

  $O_{2n}^{p}(k)=2^{p}k \bmod (2n-1)$.

- Since r is the smallest number such that

  $2^{r} = 1 \bmod (2n-1)$,

  this implies that $O_{2n}^{r}(k)=k \bmod (2n-1)$.

- Hence $O_{2n}^{r} = i$ and since r is the smallest number such that this is true, this implies that

  $\text{order}(O_{2n})=r$

- Note that there is no “easy” formula for the smallest r with

  $2^r = 1 \bmod (2n-1)$.

- When 2n-1 is prime, then Fermat's little theorem implies that

  $2^{2n-2} = 1 \bmod (2n-1)$.

  Hence r is a factor of 2n-2.

- In general, r is a factor of φ(2n-1) where φ is a special function called the **Euler function**.

Table: Order of perfect shuffles.

N	Order(O_N)	Order(I_N)
2	1	2
3	2	2
4	2	4
5	4	4
6	4	3
7	3	3
8	3	6
9	6	6
10	6	10
11	10	10
12	10	12
13	12	12
14	12	4
15	4	4

N	Order(O_N)	Order(I_N)
16	4	8
17	8	8
18	8	18
19	18	18
20	18	28
30	28	5
31	5	5
32	5	10
51	8	8
52	8	52
53	52	52
54	52	20

- One of the most surprising things is that order(O_{52})=8 and order(O_{53})=52.
- Just adding one extra card to a deck of cards changes the order by so much!
- In odd decks of cards, we can also prove the following generalization in a similar fashion.

The fundamental theorem of Faro shuffling (in odd decks). (Elmsley, Morris)

- Let N=2n-1 and suppose that

  $S_1, S_2, \ldots, S_m$ are perfect shuffles (out or in).

- Let

  $d(S_i)=0$ if S_i is an out shuffle; and

  $d(S_i)=1$ if S_i is an in shuffle. Then

$$S_m \circ \ldots \circ S_2 \circ S_1(k) = \left[2^m k + \sum_{i=1}^{m} 2^{m-i} d(S_i)\right] \ mod\ N$$

Proof:

- Just use the fact that

  $S_i(k) = 2p \bmod N$ if S_i is an out shuffle; and

  $S_i(k) = 2p+1 \bmod N$ if S_i is an in shuffle

  and mathematical induction.

- This theorem has an interesting corollary:
- Suppose that $2^m=1 \bmod N$, then the theorem implies that

$$S_m \circ \ldots \circ S_2 \circ S_1(k) = \left[k + \sum_{i=1}^{m} 2^{m-i} d(S_i)\right] \bmod N$$
$$= k + s \bmod N$$

- Note that s does not depend on k.

  i.e. $S_m \circ \ldots \circ S_2 \circ S_1$ is just a cut of the deck of cards!!!

- e.g. We have $2^4=1 \bmod 15$ and hence in a deck of 15 cards, *any* sequence of 4 perfect shuffles (in or out) is just a cut on the deck.
- Note that by choosing in/out shuffles appropriately, we can control the value of s.
- One “application” of this is that card cheats can pretend to shuffle the deck but all they are actually doing is cutting the deck by a known amount s!

Groups generated by perfect shuffles.

- Suppose that S and T are two shuffles in $\mathbf{S}_{52}$.
- We consider all shuffles that can be obtained from S and T

  e.g. $T \circ S$, $T \circ S \circ T$, $S^4 \circ T^2 \circ S$, ...
- The set containing all such shuffles is written as $\langle S,T \rangle$

- In fact, the set <S,T> with the operator ◦ is also a group.
- Since <S,T> is a subset of $\mathbf{S}_{52}$, we say that <S,T> is a **subgroup** of $\mathbf{S}_{52}$.
- <S,T> is called the **group generated by S and T**.

- We will be interested in the groups <C,O>, <C,I> and <I,O> where I and O are the in and out perfect shuffles and C is the shuffle:

  $C(k)=k+1 \bmod N$

  i.e. C puts the top card on the bottom.

- Note that any cut of the deck corresponds to C^r for some r.

Theorem (Golomb)

- If N is even,

  $\langle C,O \rangle = \langle C,I \rangle = \mathbf{S}_N$.

  In other words any shuffle of a deck of N cards can be replicated using only cuts and out shuffles or cuts and in shuffles.

- If N is odd,

  $\langle C,O \rangle = \langle C,I \rangle = \{C^p \circ O^r : r,p=1,2,\ldots\}$

  In other words, the shuffles in <C,O> and <C,I> can be replicated by out shuffling the deck a number of times and then cutting the deck.

- This theorem implies that in a deck of 52 cards, all $52! \approx 80.7 \times 10^{66}$ shuffles can be replicated using only cuts and out shuffles.

  But if we remove just one card, then only $51 \times 8 = 408$ shuffles can be obtained using cuts and out shuffles!

- One card makes such a huge difference!!
- From this theorem, and the Fundamental Theorem of faro shuffling, we obtain the following theorem on <O,I> for odd decks.

Theorem (Golomb)

- If N is odd,

  $\langle O,I\rangle=\langle C,O\rangle=\langle C,I\rangle=\{C^p\circ O^r: r,p=1,2,\ldots\}$

- It only remains to consider <O,I> in even decks. It turns out that this case is considerably more complicated (requiring knowledge of graduate level algebra or more!)
- We first need the following concept:

Isomorphism

- Often in group theory, we are not interested in the actual contents of the group (shuffles, numbers, ...) but rather the overall structure of the group.
- We say two groups **F** and **G** are **isomorphic** if they have the same structure.

- In 1981, Diaconis, Graham and Kantor published a paper which classifies <O,I> up to isomorphism for even decks.
- We will only state a few highlights.

Table: Number of elements in <O,I>.

N=2n	|<O,I>|
2	2
4	$2 \cdot 2^2$
6	M/2
8	$3 \cdot 2^2$
10	M/2
12	M/(3!)
14	M/2
16	$4 \cdot 2^2$
18	M/2
20	M
22	M/2
24	(M/2)·(7!)

N=2n	|<O,I>|
26	M/2
28	M
30	M/2
32	$5 \cdot 2^2$
34	M/2
36	M
38	M/2
40	M/4
42	M/2
44	M
46	M/2
48	M/4

- $M=n!2^n$

Theorem (Diaconis, Graham, Kantor)

- If n = 2 mod 4 and n>6, then <O,I> is isomorphic to the Weyl group B_n.
- If n = 6 (N=12), then <O,I> is the semidirect product of $\mathbf{Z}_2^6$ and PGL(2,5).
- If n = 1 mod 4, <O,I> is the kernel of the projection of the signature onto the Weyl group B_n.
- ...
- If n= 12 (N = 24), then <O,I> is the semi-direct product of $\mathbf{Z}_2^{11}$ and the Mathieu group of degree 12.

- What is the Mathieu group?
- Just like primes are the building blocks of whole numbers, certain groups can be thought of as the building blocks of other groups.
- These groups are called the simple groups.
- In the previous century, there was a huge research effort put into classifying all simple groups. This was completed in 1982.
- Basically, any simple group either belongs to one of 3 infinite classes or is one of 26 exceptions.

- These exceptions are called the **sporadic groups** .
- The 5 Mathieu groups are 5 of these 26 sporadic groups.
- For N=24, why is <O,I>, the group generated by the in and out perfect shuffle related to one of the Mathieu groups?

THE END.

- Thank you for listening.
- Any questions?