# Card Shuffling as a Group and the Faro Shuffle

Anna Golden, Emma Meaney, Lise Wall, Lydia Costello

## Introduction

In this poster we look at card shuffling a deck of cards is as a group. First, we establish that shuffling is a group and that it is isomorphic to the group of permutations $S_N$ where $N$ is the number of cards in a deck, typically 52 in a standard deck. We then discuss a specific type of shuffle known as the Faro or Perfect Shuffle used by magicians and gamblers, that has interesting properties when considered as a group. We prove the Fundamental Theorem of Faro Shuffling. We discuss the generating set of shuffles. We give an example of a card trick that applies these concepts.

## Why Is Card Shuffling a Group?

The set of all shuffles can be represented by the symmetric group $S_N$, where N is the number of cards in the deck.Let S be a card shuffle that acts on $S_{52}$, such that S:1,2,...,52 ↦ 1,2,...,52 (Let T, U also be shuffles on $S_{52}$). The shuffling function is a form of permutation. Card shuffling is a group because it satisfies the group axioms as follows:

- **Closure:** consider shuffles (permutations) S,T, then S ∘ T is also a shuffle (perform T, followed by S)
- **Identity:** This consists of the shuffle which leaves each element in it's original position. Let i(x) be the identity shuffle performed on x ∈ 1,2,...,52, then i(1)=1, i(2)=2,...,i(52)=52.
- **Inverse:** Each permutation S also has an inverse $S^{-1}$ contained in the group, e.g if S(1)=52, $S^{-1}(52)$=1.
- **Associative Property:** For shuffles S,T,U it is true that:
  - S ∘ (T ∘ U) = (S ∘ T) ∘ U.

## Faro/Perfect Shuffle

The Faro shuffle is a method of "perfectly" shuffling a deck of cards. A deck of cards is divided into two equal piles and then perfectly interwoven. There are two ways of doing this:

- **In Shuffle:** The In Shuffle leaves the top and bottom card second from top and bottom respectively.

$$\begin{pmatrix} 1 & 2 & 3 \dots 25 & 26 & 27 \dots 50 & 51 & 52 \\ 2 & 4 & 6 \dots 50 & 52 & 1 \dots 47 & 49 & 51 \end{pmatrix} \tag{1}$$

- **Out Shuffle:** The Out Shuffle leaves the top and bottom card in place.

$$\begin{pmatrix} 1 & 2 & 3 \dots 25 & 26 & 27 \dots 50 & 51 & 52 \\ 1 & 3 & 5 \dots 49 & 51 & 2 \dots 48 & 50 & 52 \end{pmatrix} \tag{2}$$

By doing a Faro shuffle on a memorized deck, one can always compute where a card in any given position will end up. What is perhaps more interesting is that Faro shuffles form a subgroup and will always return to the identity within a set number of shuffles. As we will see, for a deck of 52 cards, it will take exactly eight Faro Shuffles to return the cards to their original positions (i.e. $\text{Faro}^8 = id_{52}$).

## The Fundamental Theorem of Faro Shuffling

Alex Elmsley found that a series of in and out shuffles can be used to bring the original top card (at position 0) to any desired position p in the deck. This can be achieved by expressing p in binary with 0 meaning an out shuffle and 1 meaning an in shuffle. For example to go from 0 to position 7 (where 7 = 111), perform in, in, in.

With a deck of $2n$ cards, $r$ exists such that $2^{r-1} < 2n \leq 2^r$.
Where $0 < p < 2n-1$, let $t = \frac{(p+1)2^r}{2n}$.
For $p = 0$, set $t = 0$. For $p = 2n-1$, set $t = 2^r - 1$.
Express t in binary as $t = t_{r-1}t_{r-2}...t_1t_0$ with $t_i = 1$ or 0
Let s be correction terms where $s = 2nt - 2^r p = s_{r-1}s_{r-2}...s_1s_0$ with $s_i = 1$ or 0
The shuffling sequence is $t_{r-1} + s_{r-1}, t_{r-2} + s_{r-2}, ..., t_0 + s_0$

For example, if $2n = 52, p = 35$. Then $r = 6$, $t = \frac{36(64)}{52} = 44 = 101100$ and $s = 2288 - 2240 = 48 = 110000$.
Now the co-ordinate sum of 101100 and 110000 is 011100 which is out, in, in. We can ignore the final two shuffles as they do nothing to the top card.

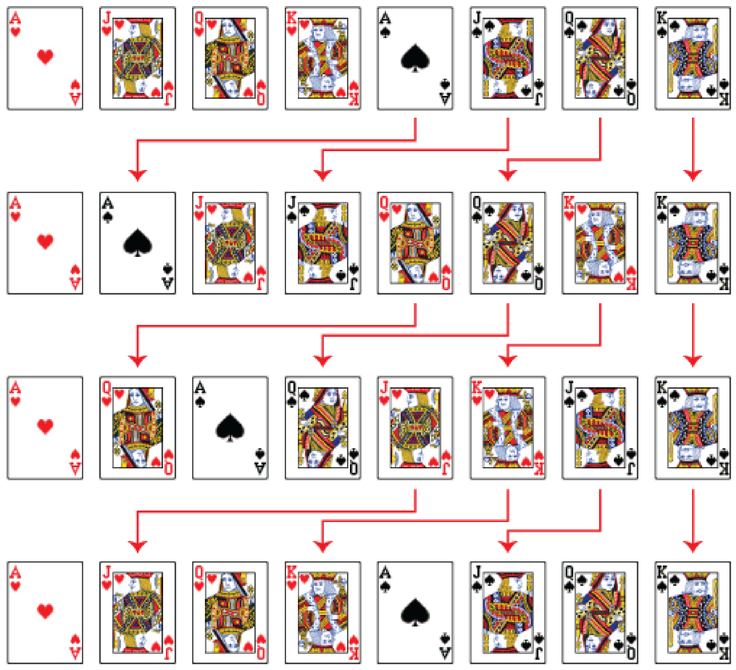

Fig. 1: For an 8-card deck, only three out-shuffles are required to restore the original order

## The Generating Set of Shuffles

Starting with a randomly shuffled deck of 52 cards, any other shuffle of the deck can be reached by a combination of swapping the first two cards and putting the bottom card on top of the deck. In other words $S_{52}$ is generated by the transposition (1 2) which swaps the first two cards in the deck and the 52-cycle (1 2 ... 52) which brings the bottom card of the deck to the top.
Proof:

Let x = (1 2 ... 52)

$$\begin{aligned}
&x(1 \quad 2)x^{-1} = (2 \quad 3) \\
&x(2 \quad 3)x^{-1} = (3 \quad 4) \\
&\vdots \\
&x(50 \quad 51)x^{-1} = (51 \quad 52) \\
&\implies (i \quad i+1) \in \langle (1 \quad 2), x \rangle \quad \forall \quad 1 \leq i \leq 51 \\
&(2 \quad 3)(1 \quad 2)(2 \quad 3)^{-1} = (1 \quad 3) \\
&(3 \quad 4)(1 \quad 3)(3 \quad 4)^{-1} = (1 \quad 4) \\
&\vdots \\
&(51 \quad 52)(1 \quad 51)(51 \quad 52)^{-1} = (1 \quad 52), \\
&\implies (1 \quad i) \in \langle (1 \quad 2), x \rangle \quad \forall \quad 1 \leq i \leq 52 \\
&\text{For any} \quad 1 \leq i < j \leq 52 : \\
&(i \quad j) = (1 \quad i)(1 \quad j)(1 \quad i)^{-1} \in \langle (1 \quad 2), x \rangle.
\end{aligned}$$

Therefore $\langle (1,2), x \rangle$ generates all transpositions in the group $S_{52}$, and so generates the group itself as every permutation is a product of transpositions.

## A Card Trick to Try

Before you start memorise the card on the bottom of the deck. Ask your friend to pick a card out of the deck, look at it and put it on top of the deck without you seeing it. Then allow them to cut the deck as many times as they want. Spread the cards out face up and announce the chosen card which is the card in front the "bottom card" you had memorised.
Why does this work?
Under the action of cutting the cards the adjacency of pairs of cards is preserved. The group H is the subgroup of $S_{52}$ generated by the 52 cycle (1 2 3... 51 52). The adjacency of pairs of cards is not changed by any action in H and so although H seems to be shuffling the cards, the chosen card will always remain in front of the original bottom card making it is easy to find the chosen card.

## References

Conrad, K.,Generating Sets. University of Conneticut.https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf
C-for-dummies.com.2017.The Perfect Shuffle | C For Dummies Blog.[online]https://c-for-dummies.com/blog/?p=2519
Diaconis, P., Graham, R. and Kantor, W.(1983). The mathematics of perfect shuffles. Advances in Applied Mathematics, 4(2), pp.175-196.
Diaconis, P. and Graham, R.(2020). The Solutions To Elmsley'S Problem.https://statweb.stanford.edu/~cgates/PERSI/papers/pre-elmsley.pdf
Ensley, D. (1999). Invariants under Group Actions to Amaze Your Friends. Mathematics Magazine, [online] 72(5), p.383.https://www.maa.org/sites/default/files/269079545577.pdf
Quinlan, R. (2020), "The Axioms of a Group", *MA3343: Groups*, available: http://www.maths.nuigalway.ie/~rquinlan/groups/section1-2.pdf [accessed 11 Dec 2020]