Periodicites and other Properties of Faro Shuffles

First Year Exploration Lab, Prof. David Fried[1]

[1]Program in Mathematics for Young Scientists, Boston University

August 21, 2023

Abstract

Faro shuffles (or Riffle shuffles) are cards that are perfectly interweved that can be categorized into infaro and outfaro shuffles. Modular equations for the periods of the card's position after performing a infaro or outfaro shuffle are presented, and the infaro case is proven. Breifly, basic combinatorics of faro shuffles are also elucidated. The main theorem presented is $2^{\epsilon} \equiv 1 \mod (n-1)$ where ϵ is the period of a card, and this is proven through traditional and spectral graph theory methods using an adjacency matrix. Extensions of the problem, including flipping the cards throughout the shuffles and then finding new modular equations.

Contents

1 Introduction

This project delves into the well discussed problem of faro shuffles and how we can look at them using varioous tools of mathematics.

Perfect Faro Shuffle: A shuffle in which the deck is separated into two half and weaved in one by one.

We can split this definition into two parts...

- **Infaro Shuffle:** The original bottom card goes to second to bottom and the top card goes to second.
- **Outfaro Shuffle:** The original bottom and top card stay the same.

Imagine you have a subset of the 52 cards given in a regular deck in a certain order. Now perform one of the perfect shuffles consistently on that subset. How long will it take for the deck to come back to the original order? This is equivalent to finding the period of the shuffle.

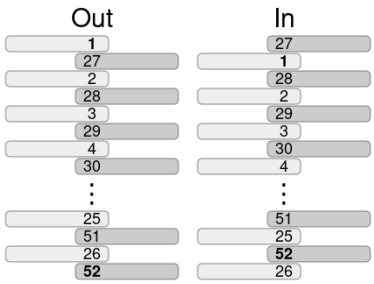


Figure 1: Diagram of a faro shuffle with 52 cards

We wanted to figure out the relation between the period of the cards and the type of perfect shuffles (infaro and outfaro). We also ventured into the areas of matrices and combinatorics.

2 Modular Equations

First observation we can make is that each of the shuffle can be defined as such where x is the initial position, n is the number of cards, and $f(x)$ gives the final position

Initial Position	Final Position
2	4
6	12
13	26
23	46
31	11
35	19

Figure 2: Left column has initial position of a card number, and this gives motivation for the infaro shuffle modular equation. This was mod 52 since we have 52 cards.

Infaro Shuffle:

$$f(x) = 2x \pmod{n+1} \tag{1}$$

Outfaro Shuffle:

$$f(x) = 2x - 1 \pmod{n-1} \tag{2}$$

We used a Python program to gather general data on the patterns found in the In-faro and Out-faro shuffles.

Number of Cards	2	4	6	8	10	12	14
Out-faro Period	1	2	4	3	6	10	12
In-faro Period	2	4	3	6	10	12	14

Table 1: This is the periods of the infaro and outfaro shuffles for a smaller number of cards. We corroborated the Python program by doing these by hand.

We see that the period number of the Out-faro and In-faro shuffles are seemingly "shifted" from each other

M-handed Shuffles

- What if instead of splitting the cards into two decks and shuffling them, we split them into 3 decks?

- We see that as we are splitting the cards into 3 decks, 3 divides the number of cards.
- We "adapt" the position functions of the Out-faro and In-faro shuffles:

  Out-faro: $f(x) \equiv m(x-1)+1 \pmod{(n-1)}$

  In-faro: $f(x) \equiv mx \pmod{(n+1)}$

  Where x is the original position, m is the number of deck splits, n is the number of cards, and $f(x)$ is the final position.

Let's prove the in faro modular equation so we can use this in further sections. A proof sketch will be provided below.

Proof. We initially start with a deck of m cards and then d partitions and then we can lay out the portions from 0 to d.

So the 0th card of the kth partition would be the kth card of all the deck. Cards with index of 1 are d, and then index 2 is $2d$, index 3 is $3d$, etc.

A card with a index of k', has position $n + dk'$ and we write $k' \equiv k \mod \frac{m}{d}$. So $k_0 = \frac{m}{d}q + k'$.

There are $\frac{m}{d}$ cards in each partition, and therefore the k_0th card's position is ...

$$\lfloor \frac{k_0}{\frac{m}{d}} \rfloor$$

From this we get...

$$k_1 = n + 2k' = \frac{k_0}{\frac{m}{d}} + d(k_0 - \frac{m}{d}q)$$

From this, with some algebraic manipulation we can get the relation, $f(x) \equiv dx \pmod{(n+1)}$

□

We can find an alternate representation including the period, ϵ, of the cards in a faro shuffle.
We let the period be ϵ and we have $2^\epsilon \equiv 1 \mod (n-1)$.

$$2^k x - (2^k - 1) = x$$

Rearranging, we get

$$1 - 2^k = x - 2^k x$$

Taking out the x on the RHS

$$1 - 2^k = x(1 - 2^k)$$

Divide both sides by $1 - 2^k$

$$x = 1 \mod (n-1)$$

This is what we wanted to show.

The equation $2^\epsilon \equiv 1 \mod (n-1)$ looks like Fermat's Little Theorem which states $a^{\phi(n)} \equiv 1 \mod (m)$ where $(a, m) = 1$.

3 Combinatorics and Graph Theory

If we have n cards then there are a total of n! to order them.

Extra Question: With 52! total random shuffles would it be possible to create a completely random shuffle with just combinations of the two perfect shuffles that we are given?

Observations

- Now quite generally, if we want to split the deck into k piles where we have n of the 52 cards then we can write $((\frac{n}{k}!)^k$. If k doesn't evenly divide n we can floor the equation such that we can have a integer factorial, we get $((\lfloor \frac{n}{k} \rfloor !)^k$
- Some other things to think about... When we have a starting sequence of 12345678. We have one strictly increasing sequence. After one perfect shuffle we get 16237845 which has 2 strictly increasing sequences. How many strictly increasing sequences can we see? It might double?
- It might double because each previous increasing sequence has two decks to go into.

A1	A	2	3	4	5	6	7	8
A2	5	A	6	2	7	3	8	4
A3	7	5	3	A	8	6	4	2
A4	8	7	6	5	4	3	2	A
A5	4	8	3	7	2	6	A	5
A6	2	4	6	8	A	3	5	7
A7	A	2	3	4	5	6	7	8

Figure 3: This is the chart of the permutations of cards after performing in faro shuffles for 8 cards. The middle red sequence of numbers is where the numbers have flipped.

A1	A	2	3	4	5	6	7	8	9	10
A2	6	A	7	2	8	3	9	4	10	5
A3	3	6	9	A	4	7	10	2	5	8
A4	7	3	10	6	2	9	5	A	8	4
A5	9	7	5	3	A	10	8	6	4	2
A6	10	9	8	7	6	5	4	3	2	A
A7	5	10	4	9	3	8	2	7	A	6
A8	8	5	2	10	7	4	A	9	6	3
A9	4	8	A	5	9	2	6	10	3	7
A10	A	2	3	4	5	6	7	8	9	10

Figure 4: Same as Figure 2, but for 10 cards.

Theorem 1: If we have $2n$ cards for some n, then after n shuffles the order of the cards at the $(n+1)k$ position reverses.

Symmetry:

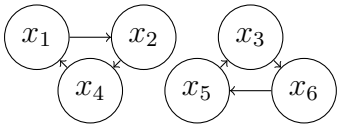
A1	A	2	3	4
A2	3	A	4	2
A3	4	3	2	A
A4	2	4	A	3
A5	A	2	3	4

Figure 5: This is a chart of the in faro shuffle for 4 cards, notice if we draw a vertical line the chart is symmetric.

With a_1 and a_m as intital and final steps then for all a_j and a_k then $j+k=m+1$, a_j and a_k follow a symmetric pattern around the center line that splits the picture vertically. The symmetric pattern is such that the cards a_j and a_k are of equal distance from the center line.

3.1 Spectral Graph Theory

We can prove the validity of $2^\epsilon \equiv 1 \mod (n-1)$ using spectral graph theory methods.



The adjacency matrix for the graph above: $A(X_6) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$

General Adjacency Matrix Formula for In-Faro:

$$A_{i,j}(X_n) = \begin{cases} 1 & \text{if } j = 2i \pmod{n+1} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

- Defining such matrix allows you to power this matrix to the kth power to shuffle the deck k times.

- And using the fact that $2^\epsilon \equiv 1 \pmod{n+1}$, we notice that $A^{\epsilon+1} = A$ where $A = A(X_n)$
- In fact, we can show that $A^\epsilon = I$ where I is the identity matrix. Since A is always a permutation matrix, we can use the fact that the eigenvalues of A is contained in the set of unity.
- If we have eigenvalue λ of A, then $\lambda, \lambda^2, \lambda^3, ..., \lambda^\epsilon$ are all eigenvalues and by rearranging (since this is repeated), we can make $\lambda^\epsilon = 1$.
- Assuming eigenvector $\vec{v}$ exist for A, $A\vec{v} = \lambda\vec{v}$
  - So, $A^2\vec{v} = \lambda\lambda\vec{v} = \lambda^2\vec{v}$ a 39928858nd by continuing to raise λ like this ϵ, we get $A^\epsilon\vec{v} = \lambda^\epsilon\vec{v} = \vec{v}$.
- Therefore, $A^\epsilon = I$

4 Extensions

We looked at a sub problem of the Faro shuffles, which is just to find the modular equations of their period. An extension of this problem would be to flip the cards as you put them down instead of putting them down as they are and seeing what the period would be.

5 Acknowledgements

Thank you to our counselor Lee Trent and our professor David Fried for guiding us through the process of Exploration. Thank you to the PROMYS Program for being able to give us this oppotunity.