

An Analysis of Riffle Shuffles

Tong Chen

March 11, 2020

1 Definition

How many shuffles are required to bring a deck of cards close to random? Before talking about how to shuffle, how to define a suit is random?

Definition 1. *One suit is called **shuffled** if and only if the probability of every permutation is equal.*

And now we analyze the most commonly used method of shuffling cards called the ordinary riffle shuffle. This involves cutting the deck approximately in half, and interleaving the two halves together. In general, a permutation π of n cards made by a riffle shuffle will have exactly 2 rising sequences unless it is the identity. Conversely, any permutation of n cards with 1 or 2 rising sequences can be obtained by a physical riffle. Thus the mathematical definition of a *riffle shuffle* is "a permutation with 1 or 2 rising sequences". Suppose c cards are initially cut off the top. Then there are $\binom{n}{c}$ possible riffle shuffles(1 of which is the identity). Finally, the total number of possible riffle shuffles is

$$1 + \sum_{c=0}^n \left(\binom{n}{c} - 1 \right) = 2^n - n$$

The following model for random riffle shuffle, suggested by Gilbert and Shannon(1955) and Reeds(1981), is mathematically tractable and qualitatively similar to shuffles done by simple card players.

Definition 2. *(1st description). Begin by choose an integer c from $0,1,\dots,n$ according to the binomial distribution $P\{C = c\} = \frac{1}{2^n} \binom{n}{c}$. Then, c cards are cut off and held in the left hand, and $n-c$ cards are held in the right hand. The cards are dropped from a given hand with probability proportional to packet size. Thus, the chance that a card is first dropped from the*

left hand packet is c/n . If this happens, the chance that the next card is dropped from the left packet is $(c-1)/(n-1)$.

There are two other descriptions of this shuffling mechanism that are useful.

Definition 3. (2nd description). Cut an n card descriptions according to a binomial distribution. If c cards are cut off, pick one of the $\binom{n}{c}$ possible shuffles uniformly.

Definition 4. (3rd description). This generates π^{-1} with the correct probability. Label the back of each card with the result of an independent, fair coin flip as 0 or 1. Remove all cards labelled 0 and place them on top of the deck, keeping them in the same relative order.

2 Analysis

The idea here is to consider shuffling as inverse sorting. The argument works for any symmetric method of labelling the cards. We know that the worst case of sorting is $\Theta(n \log n)$. And the minimum operation for riffle shuffle is $\Theta(\log n)$.

According to Trailing the Dovetail Shuffle to Its Lair written by Dave Bayer and Persi Diaconis, we can get the conclusion: 6-8 times shuffling make the suit random. Here, if S_n is the symmetric group, U the uniform probability [so $U(\pi) = 1/n!$] and Q^m the Gilbert-Shannon-Reeds probability after m shuffles, then the total variation distance is defined as

$$\|Q^m - U\| = \max_{A \subset S_n} |Q^m(A) - U(A)|$$

Table 1 gives the total variation distance for 52 cards. Table 1 shows that the total variation distance stays essentially at its maximum of 1 up to 5 shuffles, when it begins to decrease sharply by factors of 2 each time. This is an example of the cutoff phenomena described by Aldous and Diaconis (1986).

表 1: Total variation distance for m shuffles of 52 cards										
m	1	2	3	4	5	6	7	8	9	10
$\ Q^m - U\ $	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043

3 Reference

1. Bayer D , Diaconis P . Trailing the Dovetail Shuffle to its Lair[J]. The Annals of Applied Probability, 1992, 2(2):294-313.

2. David, Aldous, Persi, et al. Shuffling Cards and Stopping Times[J]. The American Mathematical Monthly, 1986.