SHUFFLING 4 CARDS: THREE SHUFFLES IS ENOUGH

Given a deck of 52 cards which begins in some fixed order, if we shuffle the deck one time it is definitely not in a completely random order. What we see after one shuffle is that there is one increasing subsequence of cards that were in the left hand and a second that comes from the cards that were in the right hand. While those two sequences of cards might be interlaced, we easily see a pattern in the way the cards appear and can even reconstruct in which order they fell from the left and right hand.

Example:

Even shuffling the deck two or three times there are still significant patterns, so much so that if you take a card out of its place and put it somewhere else in the deck after 3 shuffles someone else can probably determine look at the deck and still determine what card was displaced.

After 4 or 5 shuffles a deck of 52 cards begins to get random and in a paper in 1992, Beyer and Diaconis showed that it takes 7 shuffles to really shuffle the deck well. Their theorem may simply be stated as "seven shuffles is enough to make the deck sufficiently random" and this is the conclusion from a very precise mathematical statement.

In this article we will take a look at a rough idea of the result that Beyer and Diaconis showed to see why they conclude that we need to shuffle the deck seven times before it is random.

To try to understand their result we will look at what happens on a deck of 4 cards. We will show that for a deck of 4 cards, three shuffles is sufficient.

Say that we shuffle a deck of 4 cards using a model where we split the deck into two cards in each hand and then if there are a cards in the left hand and b cards on the right then with probability $\frac{a}{a+b}$ a cards falls from the left hand and with probability $\frac{b}{a+b}$ a card falls from the right. After one shuffle there are only 6 possible orderings of the deck but after two shuffles already all possible orderings of the deck are possible (although some orderings are more likely than others).

Below is a table of probabilities for each permutation of the cards 1 through 4 the probability after k shuffles of this type (with $0 \leq k \leq 4$) of a particular ordering of the cards arising. These are probability distributions for the set of permutations on 4 letters.

If you look in the table below you see that the permutation 3142 appears in the distribution for one shuffle of the 4 card deck, $Shuf^1$, with probability 1/6. The reason for this is that we take the deck 1234 split it in two so that 12 is in the left hand and 34 is the right. Now 3 falls first with probability $2/(2+2) = 1/2$, then 1 falls from the left hand with probability $2/(2+1) = 2/3$ and then 4 falls from the right hand with probability $1/(1+1) = 1/2$ and finally the 2 is the last card to fall.

The probability for the other five orders 1234, 1324, 1342, 3124 and 3412 that may be obtained after one shuffle can be calculated in a similar manner and for each of them we find that their probability is also 1/6.

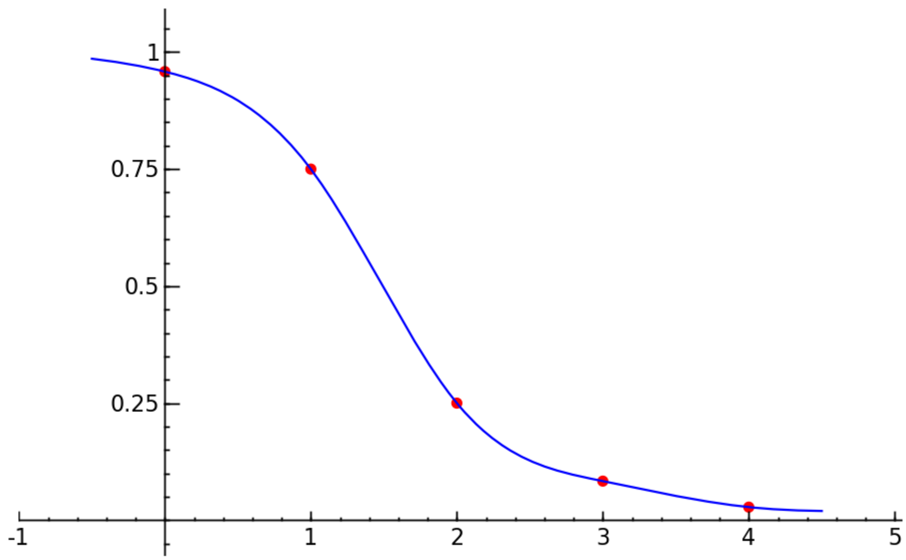
order	$Shuf^0$	$Shuf^1$	$Shuf^2$	$Shuf^3$	$Shuf^4$
1234	1	1/6	1/12	1/18	5/108
1243	0	0	1/36	1/27	13/324
1324	0	1/6	1/12	1/18	5/108
1342	0	1/6	1/12	1/18	5/108
1423	0	0	1/36	1/27	13/324
1432	0	0	1/36	1/27	13/324
2134	0	0	1/36	1/27	13/324
2143	0	0	1/36	1/27	13/324
2314	0	0	1/36	1/27	13/324
2341	0	0	1/36	1/27	13/324
2413	0	0	1/36	1/27	13/324
2431	0	0	1/36	1/27	13/324
3124	0	1/6	1/12	1/18	5/108
3142	0	1/6	1/12	1/18	5/108
3214	0	0	1/36	1/27	13/324
3241	0	0	1/36	1/27	13/324
3412	0	1/6	1/12	1/18	5/108
3421	0	0	1/36	1/27	13/324
4123	0	0	1/36	1/27	13/324
4132	0	0	1/36	1/27	13/324
4213	0	0	1/36	1/27	13/324
4231	0	0	1/36	1/27	13/324
4312	0	0	1/36	1/27	13/324
4321	0	0	1/36	1/27	13/324

We compare these to the uniform probability distribution which is defined by $U(\pi) = 1/24$ for all permutations π of the 4 cards. We compare $Shuf^k$ to U by calculating the value

$$||Shuf^k - U|| = \frac{1}{2}\sum_{\pi} |Shuf^k(\pi) - U(\pi)|$$

and we find that the distances between the ordered deck and the uniform distribution is $||Shuf^0 - U|| = 23/24$, the distance between one shuffle and the uniform distribution is $||Shuf^1 - U|| = 3/4$, between two shuffles and the uniform distribution is $||Shuf^2 - U|| =$

1/4, between three shuffles and the uniform distribution is $||Shuf^3 - U|| = 1/12$ and between four shuffles and the uniform distribution is $||Shuf^4 - U|| = 1/36$.



While it is clear that the $Shuf^4$ is closer to the uniform distribution than $Shuf^3$ (by a factor of 3) already the distance between the distributions is probably small enough to consider them sufficiently shuffled and hence we conclude "three shuffles is enough" for a deck of of 4 cards.

This is precisely what Beyer and Diaconis did for a deck of 52 cards which allowed them to conclude that "7 suffles is enough" for a similar distribution on a 52 card deck that had a few minor differences. The mathematical model that they studied did not assume that the deck was first split into two equal parts. Instead they said that the probability that there are r cards in the left hand will be

$$\frac{\binom{52}{r}}{2^r} .$$

If we think that this mathematical model of shuffling should correspond to the way that humans really shuffle a deck of cards, this assumption seems realistic because with this definition the probability that a shuffler starts with between 24 and 28 cards in each hand is slightly greater than 50% and when r is larger than 28 or smaller than 24 the probability that the shuffler begins with r cards is generally fairly small.

It is an interesting question if the mathematical model that Beyer and Diaconis studied really does correspond to the real way that people shuffle cards. It could be that the model that they studied in the theorem is not at all related to the real way that people shuffle cards. So it is a completely separate question if the assumptions that they made about the model of shuffling corresponds to real world shuffling. Diaconis did additional experiments by asking lots of people to shuffle a deck of cards and he studied the results to see if it did match his model. Fortunately the results of those experiments did show that reality and the mathematical model were closely related.

There are two places in the theorem of Beyer and Diaconis where some degree of arbitrariness exists in the conclusion that it was sufficient to stop shuffling the deck after seven times. The The cutoff value for where we decide that the distance between two distributions is “small enough” was somewhat arbitrary and Beyer and Diaconis concluded that this they needed seven shuffles instead of six because the difference between the uniform distribution and six shuffles still seemed too large while for seven shuffles the cutoff was smaller.

The other calculation that was slightly arbitrary about this conclusion is the formula that we used to measure the distance between the the shuffle distribution and the uniform distribution. There are other formulas for the distance between two distributions. Instead we could have taken as a measure the following formula

$$||Shuf^k - U||_2 = \sqrt{\frac{1}{2}\sum_{\pi}(Shuf^k(\pi) - U(\pi))^2}\ .$$

In this case $||Shuf^1 - U||_2 = 1/4$, between two shuffles and the uniform distribution is $||Shuf^2 - U||_2 = 1/12$, between three shuffles and the uniform distribution is $||Shuf^3 - U||_2 = 1/36$ and between four shuffles and the uniform distribution is $||Shuf^4 - U||_2 = 1/108$. So using this measure and the same reasoning we could conclude that really “two shuffles is enough.” Which answer is correct? Well, this is where a degree of arbitrariness exists in deciding what the mathematics means.

This is exactly what happened in 2000. In an article by L. Trefthen, he concluded that by using a different measure of the difference of distributions then after six shuffles the deck is sufficiently shuffled.

Exercises:

(1) Say that you have cards 1-5 in your right hand and cards 6-10 in your left and they fall from either your right or left with probability in the model described above (that is, if there are a cards in the left hand and b in the right then a card falls from the left hand with probability $\frac{a}{a+b}$ and from the right hand with probability $\frac{b}{a+b}$). What is the probability that the order of the cards is 1 2 3 4 6 7 8 9 5 10 after one shuffle? What is the probability that it is 1 6 2 7 3 8 4 5 9 10?

(2) After completing the previous problem, make a conjecture for the probability of a given permutation arising from the procedure of splitting the deck perfectly in two and then cards fall with respect to the probability of a shuffle.