Introduction

Shuffling a deck of playing cards is a very important life skill. The standard riffle shuffle goes like this: you take a stack of cards, split it into two piles, hold one pile in your left hand and the other in your right, and drop cards from each hand onto a common pile on the table in random order. After repeating this several times, your card deck is hopefully fairly well-mixed and ready for a game or maybe a magic trick. (Of course, in practice, the easiest way to perform the riffle shuffle is to allow the cards to interleave without dropping them, but this is mathematically equivalent.)

People often perform only three or four riffle shuffles in a row before using a standard deck of 52 playing cards. One might ask if this is really enough. It's not hard to see that after one riffle shuffle, many orderings of the cards are impossible to reach and many others are much more likely than they ought to be in a uniformly random probability distribution. How many shuffles in a row do you really need to approximate uniform randomness? This Power Round builds up some of the basic ideas you need to answer this question.

In order to understand how to mathematize shuffling, we first discuss the basic concept of a permutation and some specific properties that we will need. Next, we give a mathematically precise definition of the Gilbert-Shannon-Reeds riffle shuffle, which has been shown in experiments to be a good model for how real people shuffle, and develop the theory of the probabilities it generates. Unfortunately, actually computing the necessary number of shuffles for approximate uniform randomness is beyond the scope of this test, but hopefully you will come to believe that such a number is indeed computable. Finally, we develop the mathematics of the perfect shuffle, a deterministic shuffle very useful in magic tricks to those able to perform it. Have fun!

Permutation Enumeration

One of the key tools that we will use to analyze shuffles is the **permutation**. A permutation of a set S is defined as a *listing* of elements of S in some order (with each element appearing precisely once); for example, permutations of $S = \{1, 2, 3, 4, 5\}$ include $(4, 2, 3, 5, 1)$ or $(3, 2, 1, 4, 5)$.

1. (a) List all permutations of $\{1, 2, 3\}$.
   (b) Give an expression for the number of permutations of $\{1, 2, 3, \ldots, n\}$ in terms of n. Compute the number for $n = 5$.

We can also think of a permutation as an *operation* or a *process* that we perform on some ordered listing to get another ordered listing. For instance, with $S = \{1, 2, 3\}$, we can think of the permutation $(2, 1, 3)$ as the operation of swapping the first and second elements in an ordered listing of three elements, and leaving the third in place. In general, we interpret a permutation $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ as the operation that sends the $\sigma(1)$th element to the first position, the $\sigma(2)$th element to the second position, and so on. The listings we previously wrote down are just what we get when we apply the permutation to $(1, 2, \ldots, n)$. Note that the permutation whose listing is itself $(1, 2, \ldots, n)$ corresponds to doing nothing at all—for this reason, we call it the **identity permutation**, and write it as 1.

Given this interpretation, we define the notions of composition and inverse. The **composition** $\sigma \circ \tau$ of two permutations σ and τ is the operation of performing τ *first*, then σ. The **inverse** σ^{-1} of a permutation σ is the permutation such that $\sigma^{-1} \circ \sigma = 1$.

2. (a) Compute the composition $\sigma \circ \tau$ of permutations $\sigma = (1, 5, 4, 3, 6, 2)$ and $\tau = (2, 4, 6, 3, 1, 5)$.
   (b) Compute the inverse of $(3, 1, 4, 2)$ and the inverse of $(2, 4, 6, 3, 1, 5)$.
   (c) Show that $(\sigma \circ \tau)^{-1} = \tau^{-1} \circ \sigma^{-1}$ for all permutations σ and τ of $\{1, 2, \ldots, n\}$.

When talking about shuffles, both of these interpretations of permutations have a natural meaning. The listing interpretation corresponds to a state of the deck, and the process interpretation corresponds to shuffling the deck form one state to another.

3. (a) Suppose that a process shuffles a deck of σ into τ. Which permutation will be produced when $(1, 2, \cdots, n)$ is shuffled by that process? Justify.

So far, we've talked about permutations as deterministic processes that always produce the same result on the same input. But in real shuffling, people usually don't produce the same result every time (unless they're trained magicians!). Thus, we will mainly focus on shuffling processes that are **random processes**, i.e. different outcomes occur with certain probabilities. The probability that a random shuffle turns a deck σ into a deck τ is called the **transition probability** from σ to τ.

4. For any random shuffle, show that the transition probability from σ to τ is same as from 1 to $\tau \circ \sigma^{-1}$.

Now, let's return to permutations. An **ascent** of a permutation σ of $\{1, 2, \ldots, n\}$ is any position $1 \leq i < n$ such that $\sigma(i) < \sigma(i+1)$. For example, the permutation $(2, 7, 1, 3, 5, 4, 8, 6)$ has ascents at positions $1, 3, 4, 6$. Similarly, a **descent** of a permutation σ is any position where $\sigma(i) > \sigma(i+1)$. In our example, the descents occur at positions $2, 5, 7$. Note that every position $i < n$ is either an ascent or a descent.

5. (a) List the ascents and descents of $(9, 2, 7, 6, 3, 1, 8, 4, 5)$.
   (b) Compute the number of permutations of $\{1, 2, 3\}$ with exactly one descent.
   (c) There are 11 permutations of $\{1, 2, 3, 4\}$ with exactly two ascents. List them.

   No explanations required.

Define the **Eulerian number** $\left\langle {n \atop k} \right\rangle$ as the number of permutations of $\{1, 2, \ldots, n\}$ with k ascents. For example, as given in the preceding problem, $\left\langle {4 \atop 2} \right\rangle = 11$.

6. Prove the symmetry property of Eulerian numbers:

$$\left\langle {n \atop k} \right\rangle = \left\langle {n \atop n-k-1} \right\rangle.$$

7. Prove that the Eulerian numbers satisfy the recurrence

$$\left\langle {n \atop k} \right\rangle = (k+1)\left\langle {n-1 \atop k} \right\rangle + (n-k)\left\langle {n-1 \atop k-1} \right\rangle.$$

8. Using the recurrence for Eulerian numbers, compute a table of Eulerian numbers. Include $\left\langle {n \atop k} \right\rangle$ for $0 \leq k \leq n \leq 6$.

9. Prove Worpitzky's Identity:

$$x^n = \sum_{k=0}^{n} \left\langle {n \atop k} \right\rangle \binom{x+k}{n}.$$

   To ensure that the binomial coefficient makes sense, assume that x is an integer and $x \geq n$.[1]

A **rising sequence** of a permutation σ is a maximal sequence of consecutive numbers appearing as a subsequence of σ. Every permutation decomposes into disjoint rising sequences. For example, the permutation $(6, 1, 2, 4, 7, 5, 3)$ decomposes into three rising sequences: $(1, 2, 3)$, $(4, 5)$, and $(6, 7)$. Here, $(1, 2, 3)$ is a rising sequence of $(6, 1, 2, 4, 7, 5, 3)$ because the numbers 1, 2, 3 appear in order in σ but 1, 2, 3, 4 do not.

10. Recall the definition of the inverse of a permutation from the text before problem 2. Show that the number of rising sequences of a permutation σ is equal to one more than the number of descents of σ^{-1}. That is, show

$$\#\{\text{rising sequences of } \sigma\} = \#\{\text{descents of } \sigma^{-1}\} + 1.$$

[1] This actually works in greater generality. We can define generalized binomial coefficients $\binom{a}{b}$ for any real numbers a and b, and Worpitzky's identity holds in this more general context.

The Gilbert-Shannon-Reeds shuffle

As remarked in the introduction, the Gilbert-Shannon-Reeds (GSR) shuffle is a mathematical model which has been shown in experiments to fit the way real people shuffle real card decks. Here we will develop this model and a number of its interesting properties.

First we introduce some standard notation. Let $j_1, j_2, \ldots, j_a$ be nonnegative integers so that $j_1 + j_2 + \cdots + j_a = n$. We define

$$\binom{n}{j_1, j_2, \ldots, j_a} = \frac{n!}{j_1! j_2! \cdots j_a!}.$$

This number is called a multinomial coefficient. Of course, when $a = 2$, this is just a binomial coefficient, which we will usually refer to as $\binom{n}{j_1}$.

11. Compute (no explanations required):
    (a) $\binom{7}{3,2,2}$,
    (b) $\binom{8}{2,2,2,2}$, and
    (c) $\binom{100}{99,1,0,0,0}$.

The standard GSR shuffle works like this. Take a deck of n cards and cut it into a left pile and a right pile containing the bottom x cards and top y cards respectively (so $x + y = n$), in such a manner that the probability of putting x cards into the left pile is $\binom{n}{x}/2^n$. Drop cards from the bottom of either the left or the right pile one at a time, in such a manner that if at any point you're holding X cards on the left and Y cards on the right, the probability that the next card dropped comes from the left is $X/(X + Y)$.

12. Take a stack of three cards labeled $1, 2, 3$ from bottom to top and apply the GSR shuffle once. Consider the resulting pile, from bottom to top, as a permutation of $1, 2, 3$.
    (a) Are any permutations impossible to get? If so, which one(s)?
    (b) Compute the probability of putting (i) 0, (ii) 1, (iii) 2, (iv) 3 cards into the left pile during the cut.
    (c) Compute the probability of the final permutation being (i) $3, 1, 2$, (ii) $1, 2, 3$.

    No explanations required.

13. (a) In the general case with n cards, why do the given probabilities of cutting $0, 1, \ldots, n$ cards into the left pile always actually add up to 1? That is, show that $\frac{\binom{n}{0}}{2^n} + \frac{\binom{n}{1}}{2^n} + \cdots + \frac{\binom{n}{n}}{2^n} = 1$.
    (b) Take a standard deck of 52 cards and perform one GSR shuffle. Show that the probability of cutting 0 cards into one of the piles is less than one in one trillion (10^{-12}).

Now we're ready to describe the GSR a-shuffle, which is exactly like the standard GSR shuffle except with a piles. That is, take your deck of n cards, cut it into piles of size $j_1, \ldots, j_a$ with $j_1 + \cdots + j_a = n$ so that the probability of getting precisely those sizes in that order is $\binom{n}{j_1, \ldots, j_a}\frac{1}{a^n}$ (we will refer to this as the *cutting stage*), and drop cards from the piles, one at a time from the bottom, so that whenever you are holding piles of size $J_1, \ldots, J_a$ respectively, the probability of dropping the next card from the kth pile is $J_k/(J_1 + \cdots + J_a)$ (this is the *dropping stage*). In the future, we will consistently assume the following: 1. The cards start out numbered 1 to n from bottom to top. 2. The order of the cards after the dropping stage, from bottom to top, will be considered as a permutation of $1, 2, \ldots, n$.

14. (a) Take a 4-card deck and perform one 3-shuffle. Compute the probability that after the cutting stage, the pile sizes will be $1, 1, 2$ in some order.
    (b) Now suppose the same 4-card deck has already been cut into piles of size $1, 1, 2$ from left to right (so the leftmost pile has the card numbered 1, the middle pile has card 2, and the rightmost pile has cards 3 and 4). Perform the dropping stage.

(i) How many permutations of $1, 2, 3, 4$ are possible results?

(ii) Compute the probability (given this initial cut) that the final permutation is $2, 3, 4, 1$.

(iii) Compute the probability that it is $3, 2, 4, 1$.

No explanations required.

15. (a) Prove that the probabilities we've given for every possible way to cut the cards during the cutting stage really do add up to 1.

(b) Take an n-card deck which has already been cut into a piles of size $j_1, \ldots, j_a$. After the dropping stage, how many permutations of $1, \ldots, n$ are possible? Justify.

(c) Prove that, *given this initial cut*, every permutation of $1, \ldots, n$ which is possible after the dropping stage occurs with equal probability. This shows that every possible path of operation, from deck to cut piles to final permutation, occurs with probability exactly $1/a^n$. Conclude that the transition probability of the GSR a-shuffle from 1 to σ is the same as the number of paths leading to σ divided by a^n. Refer to the definitions after problem 3.

We will now describe a few apparently different shuffles which turn out to be the GSR a-shuffle in disguise, or related. The diversity of these descriptions shows just how mathematically rich the GSR shuffle is!

16. (a) A "maximum entropy a-shuffle" is any shuffle in which you cut an n-card deck into a (possibly empty) piles and then drop cards from the piles one by one, with the stipulation that every possible path from deck to piles to final permutation should be equally likely. Prove that the *only* way to satisfy this property is to use the same probabilities as in the GSR a-shuffle.

(b) A "sequential a-shuffle" works as follows. First you cut an n-card deck into a piles according to the GSR probability distribution (i.e. getting piles of size $j_1, \ldots, j_a$ occurs with probability $\binom{n}{j_1,\ldots,j_a}$). Then you shuffle pile 1 and 2 together using the dropping stage of the standard GSR 2-shuffle. Having done this, you shuffle the combined pile with pile 3, take the result and shuffle with pile 4, and so on until you have only one pile left. Prove that the probability of getting any particular permutation at the end is the same as with the standard a-shuffle.

(c) An "inverse a-shuffle" works as follows. Take your n-card deck and, *dealing from the bottom*, place each card on one of a piles uniformly at random (that is, choose each pile with probability $1/a$). Once you're done, stack the piles together in order from left to right.

(i) Show that inverse a-shuffle is not equivalent to the standard a-shuffle in general by exhibiting a permutation of 4 cards reachable by an inverse 2-shuffle which is *not* reachable by a standard 2-shuffle. Justify.

(ii) Show that the transition probability from σ to τ of the inverse a-shuffle is the same as the transition probability τ to σ of the standard a-shuffle. Refer to the definitions after problem 3.

17. (a) Prove that an inverse a-shuffle followed by an inverse b-shuffle gives rise to permutations with the same probabilities as an inverse ab-shuffle. (This is called the product rule.)

(b) Explain why this property of an a-shuffle followed by a b-shuffle being the same as an ab-shuffle must also hold when carrying out the standard (AKA maximal entropy) and sequential forms of the GSR shuffle. Justify rigorously.

18. (a) Suppose σ is a permutation with r rising sequences. Prove that the transition probability from 1 to σ for the GSR a-shuffle of an n-card deck is

$$\frac{\binom{a+n-r}{n}}{a^n}.$$

(b) Use this to give another proof of Worpitzky's identity.

(c) Use part a of this problem and Problem 17 to show that if we repeat an a-shuffle k times on the same deck, the probability of any one permutation σ appearing after the last shuffle approaches $1/n!$ as k approaches infinity.

Using the GSR model and some analysis too advanced to explain here, one can show that an n-card deck must be shuffled at least $\frac{3}{2}\log_2 n$ times before the probability distribution of the resulting permutations begins to approach uniformly random. This number is 7 for a 52-card normal playing deck and 9 for an 81-card SET deck. We here at the Rice Math Tournament consider it very important that you take this knowledge into account the next time you play a card game!

Perfect shuffles

So far, we've been discussing a method of shuffling which aims to make the resulting permutation random. For certain sorts of people, such as magicians, it is more important to discuss forms of shuffling which are perfectly predictable. Here we analyze the interesting mathematics behind one such shuffle.

In a slight departure from the notation of the previous section, we will work with a deck of $2n$ cards which starts out numbered $0, 1, \ldots, 2n-1$ from bottom to top. (This also means that we will refer to the location of the bottom card as the 0th position in the deck, and so on.) There are two perfect riffle shuffles, the out-shuffle O and the in-shuffle I. In both shuffles, you cut the deck exactly in half and alternate dropping a card from each half. O leaves the original top card on the top, whereas I leaves it second from the top. For example, applying O to $0, 1, \ldots, 2n-1$ gives $0, n, 1, n+1, 2, n+2, \ldots, n-1, 2n-1$, whereas applying I to $0, 1, \ldots, 2n-1$ gives $n, 0, n+1, 1, n+2, 2, \ldots, 2n-1, n-1$. We will refer to the permutations obtained by applying O and I to $a_0, a_1, \ldots, a_{2n-1}$ as $O(a_0, a_1, \ldots, a_{2n-1})$ and $I(a_0, a_1, \ldots, a_{2n-1})$ respectively; thus we might say that $O(0, 1, \ldots, 2n-1) = 0, n, 1, n+1, 2, n+2, \ldots, n-1, 2n-1$. We will refer to the permutation obtained by applying O to $a_0, a_1, \ldots, a_{2n-1}$ k times as $O^k(a_0, a_1, \ldots, a_{2n-1})$, and similarly for I.

The *order* of a shuffle on $2n$ cards is the least positive number of times you must apply it to $0, 1, \ldots, 2n-1$ before getting $0, 1, \ldots, 2n-1$ back.

19. Compute (no explanation needed)
    (a) $I(O(I(0, 1, 2, 3, 4, 5)))$,
    (b) the order of O on 8 cards, and
    (c) $O^k(0, 1, 2, 3, 4, 5, 6, 7)$ for all $k \geq 1$.

20. (a) Prove that after one out-shuffle of $2n$ cards, the card numbered j has moved to position $2j \pmod{2n-1}$.
    (b) Prove that the order of an in-shuffle on $2n$ cards is the same as the order (of the middle n cards) of an out-shuffle on $2n+2$ cards.
    (c) Prove that the order of an out-shuffle on $2n$ cards is the least positive integer k such that $2^k \equiv 1 \pmod{2n-1}$.
    (d) Compute the order of an out-shuffle on 52 cards.

21. (a) Take a deck of 2^m cards and number them as usual. Prove that if a card's number has binary representation $\underline{a_{m-1}a_{m-2}\ldots a_0}$, after one out-shuffle, that card has moved to position $\underline{a_{m-2}\ldots a_0 a_{m-1}}$.
    (b) What do m in-shuffles do to 2^m cards? Justify.

22. Given a deck of $2n$ cards numbered as usual and $k \in \{0, 1, \ldots, 2n-1\}$, state and prove an algorithm consisting only of in- and out- shuffles for bringing the card numbered 0 to the kth position in the deck. (Hint: consider the binary expansion of k.)