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

   Solution to Problem 1:

   (a) $(1, 2, 3)$, $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$, $(3, 2, 1)$

   (b) $n!$. 120.

We can also think of a permutation as an *operation* 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) **[2]** Compute the composition $\sigma \circ \tau$ of permutations $\sigma = (1, 5, 4, 3, 6, 2)$ and $\tau = (2, 4, 6, 3, 1, 5)$.
   (b) **[2]** Compute the inverse of $(3, 1, 4, 2)$ and the inverse of $(2, 4, 6, 3, 1, 5)$.
   (c) **[2]** Show that $(\sigma \circ \tau)^{-1} = \tau^{-1} \circ \sigma^{-1}$ for all permutations σ and τ of $\{1, 2, \ldots, n\}$.

   Solution to Problem 2:

   (a) $(2, 1, 3, 6, 5, 4)$

   (b) $(2, 4, 1, 3)$, $(5, 1, 4, 2, 6, 3)$.

   (c) We can show that $\tau^{-1} \circ \sigma^{-1}$ is the inverse of $(\sigma \circ \tau)$ as follows:

$$(\tau^{-1} \circ \sigma^{-1}) \circ (\sigma \circ \tau) = \tau^{-1} \circ (\sigma^{-1} \circ \sigma) \circ \tau = \tau^{-1} \circ \tau = 1.$$

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

   Solution to Problem 3: $\tau \circ \sigma^{-1}$. Since a permutation μ changes σ to $\mu \circ \sigma$, μ should be $\tau \circ \sigma^{-1}$ in order for $\mu \circ \sigma$ to be τ.

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

   Solution to Problem 4: The probability that a random shuffle takes σ to $\mu \circ \sigma$ depends only on μ, since changing the labels on the cards does not affect the shuffle. So we can replace σ by 1 and, according to problem 3, therefore replace τ by $\mu = \tau \circ \sigma^{-1}$ without changing the transition probability.

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

   No explanations required.

   Solution to Problem 5:

   (a) Ascents at $2, 6, 8$; descents at $1, 3, 4, 5, 7$.
   (b) 4. They are $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$.
   (c) $(1, 2, 4, 3)$, $(1, 3, 2, 4)$, $(1, 3, 4, 2)$, $(1, 4, 2, 3)$, $(2, 1, 3, 4)$, $(2, 3, 1, 4)$, $(2, 3, 4, 1)$, $(2, 4, 1, 3)$, $(3, 1, 2, 4)$, $(3, 4, 1, 2)$, $(4, 1, 2, 3)$.

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. **[5]** Prove the symmetry property of Eulerian numbers:

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

   Solution to Problem 6: We find a bijection (one-to-one correspondence) between the permutations with k ascents and the permutations with $n-k-1$ ascents. Indeed, if a permutation $\sigma = (\sigma(1), \sigma(2), \ldots, \sigma(n))$ has k ascents, then it has $n-k-1$ descents because each position $i < n$ is either an ascent or a descent. Reversing the permutation swaps ascents and descents, so therefore the permutation $(\sigma(n), \sigma(n-1), \ldots, \sigma(1))$ has $n-k-1$ ascents and k descents.

7. **[8]** Prove that the Eulerian numbers satisfy the recurrence

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

   Solution to Problem 7: Consider any permutation σ of $\{1, 2, \ldots, n\}$ with k ascents. We have $\sigma(i) = n$ for some $1 \leq i \leq n$, and removing this $\sigma(i)$ yields a permutation σ' of $\{1, 2, \ldots, n-1\}$ with either k or $k-1$ ascents.

   Every permutation of $\{1, 2, \ldots, n\}$ with k ascents is therefore built from a permutation of $\{1, 2, \ldots, n-1\}$ with k or $k-1$ ascents by inserting n. There are now two cases.

   Given a permutation of $\{1, 2, \ldots, n-1\}$ with $k-1$ ascents, we gain an ascent by inserting n only when we do so at a descent or at the end of the permutation. There are $n-k-1$ descents, so each such permutation produces $n-k$ permutations of $\{1, 2, \ldots, n\}$ with k ascents.

   Similarly, given a permutation of $\{1, 2, \ldots, n-1\}$ with k ascents, we want to preserve the number of ascents when inserting n. To do this, the insertion must happen at one of the k ascents, or at the beginning of the permutation. Each such permutation therefore produces $k+1$ permutations of $\{1, 2, \ldots, n\}$ with k ascents.

   Combining these two cases yields the desired recurrence.

8. **[5]** Using the recurrence for Eulerian numbers, compute a table of Eulerian numbers. Include $\left\langle {n \atop k} \right\rangle$ for $1 \le n \le 6$, $0 \le k \le 6$.

Solution to Problem 8:

n	$\left\langle {n \atop 0} \right\rangle$	$\left\langle {n \atop 1} \right\rangle$	$\left\langle {n \atop 2} \right\rangle$	$\left\langle {n \atop 3} \right\rangle$	$\left\langle {n \atop 4} \right\rangle$	$\left\langle {n \atop 5} \right\rangle$	$\left\langle {n \atop 6} \right\rangle$
1	1	0					
2	1	1	0				
3	1	4	1	0			
4	1	11	11	1	0		
5	1	26	66	26	1	0	
6	1	57	302	302	57	1	0

9. **[12]** 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 $x \ge n$.[1]

Solution to Problem 9: We prove this by induction. Firstly, notice that in the case $n = 0$, we have $\left\langle {0 \atop 0} \right\rangle \binom{x}{0} = 1 = x^0$.

Now, assume that $x^n = \sum_{k=0}^{n} \left\langle {n \atop k} \right\rangle \binom{x+k}{n}$. We will use this to prove Worpitzky's identity for $n+1$. We compute using the recurrence for Eulerian numbers:

$$\begin{aligned}
\sum_{k=0}^{n+1} \left\langle {n+1 \atop k} \right\rangle \binom{x+k}{n+1} &= \sum_{k=0}^{n+1} (k+1) \left\langle {n \atop k} \right\rangle \binom{x+k}{n+1} + \sum_{k=0}^{n+1} (n-k+1) \left\langle {n \atop k-1} \right\rangle \binom{x+k}{n+1} \\
&= \sum_{k=0}^{n} (k+1) \left\langle {n \atop k} \right\rangle \binom{x+k}{n+1} + \sum_{k=0}^{n} (n-k) \left\langle {n \atop k} \right\rangle \binom{x+k+1}{n+1} \\
&= \sum_{k=0}^{n} \left\langle {n \atop k} \right\rangle \binom{x+k}{n} \left[(k+1) \frac{x+k-n}{n+1} + (n-k) \frac{x+k+1}{n+1} \right] \\
&= \sum_{k=0}^{n} \left\langle {n \atop k} \right\rangle \binom{x+k}{n} \left[\frac{xn+x}{n+1} \right] = x \sum_{k=0}^{n} \left\langle {n \atop k} \right\rangle \binom{x+k}{n} = x \cdot x^n = x^{n+1}.
\end{aligned}$$

This completes the induction.

A **rising sequence** of a permutation σ is a maximal sequence of consecutive numbers appearing as a subsequence of (not necessarily adjacent entries of) σ. (Here, "maximal" means that we cannot add more numbers to the rising sequence; $(1, 2)$ and $(1, 2, 3)$ cannot both be rising sequences.) 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. **[8]** 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

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

Solution to Problem 10: If k and $k+1$ are in the same rising sequence, then their positions $\sigma^{-1}(k)$ and $\sigma^{-1}(k+1)$ must satisfy $\sigma^{-1}(k) < \sigma^{-1}(k+1)$. This means that $k+1$ starts a new rising sequence if $\sigma^{-1}(k) > \sigma^{-1}(k+1)$, i.e. if σ^{-1} has a descent at position k. Also, there is an additional rising sequence that starts at 1; this does not correspond to a descent. Hence, the number of rising sequences of σ is one more than the number of descents of σ^{-1}.

[1] This actually works in greater generality. We can define generalized binomial coefficients $\binom{a}{b}$ for any real number a and nonnegative integer 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) **[2]** $\binom{7}{3,2,2}$,

    (b) **[2]** $\binom{8}{2,2,2,2}$, and

    (c) **[2]** $\binom{100}{99,1,0,0,0}$.

    Solution to Problem 11:

    (a) 210

    (b) 2520

    (c) 100

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) **[2]** Are any permutations impossible to get? If so, list them.

    (b) **[2]** Compute the probability of putting (i) 0, (ii) 1, (iii) 2, (iv) 3 cards into the left pile during the cut.

    (c) **[2]** Compute the probability of the final permutation being (i) $3, 1, 2$, (ii) $1, 2, 3$.

    No explanations required.

    Solution to Problem 12:

    (a) Yes, $3, 2, 1$ only.

    (b) (i) 1/8, (ii) 3/8, (iii) 3/8, (iv) 1/8.

    (c) (i) 1/8, (ii) 1/2.

13. (a) **[3]** 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) **[3]** 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}).

    Solution to Problem 13:

    (a) Standard. Can be done by either quoting binomial theorem or providing combinatorial explanations.

(b) $\frac{2}{2^{52}} < \frac{1}{2^{48}} < \frac{1}{16^{12}} < \frac{1}{10^{12}}$.

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, 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) **[2]** 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) **[2]** How many permutations of $1, 2, 3, 4$ are possible results?

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

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

    No explanations required.

Solution to Problem 14:

(a) 4/9

(b) (i) 12 (ii) 1/12 (iii) 1/12

15. (a) **[5]** 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) **[5]** 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) **[7]** Prove that, *given this initial cut*, every permutation of $1, \ldots, n$ which is possible after the dropping stage occurs with equal probability. Show that therefore every possible path of operation, from deck to cut piles to final 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 from after problem 4.

Solution to Problem 15:

(a) Standard. Possible solutions are: quoting multinomial theorem, explaining combinatorial meaning, or working with induction on a.

(b) $\binom{n}{j_1,\ldots,j_a}$. The order of the cards within each pile cannot change, so they can be considered indistinguishable.

(c) Induct on n. Clear when all piles 0. Given some possible permutation, suppose WLOG the first card comes from pile 1. The probability of this permutation is then $\frac{j_1}{n}$ times the probability of the permutation with the first card removed given piles of size $j_1 - 1, j_2, \ldots, j_a$, which by the inductive hypothesis is $1/\binom{n-1}{j_1-1,\ldots,j_a}$. This is $1/\binom{n}{j_1,\ldots,j_a}$ as desired.

(Alternatively, directly compute that regardless of dropping order, the numerator must be $j_1! \cdots j_a!$ and the denominator must be $n!$.)

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) **[6]** 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

(i) the GSR a-shuffle satisfies this property and

(ii) the *only* way to satisfy this property is to use the same probabilities as in the GSR a-shuffle.

(b) **[6]** 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) **[2]** Prove that any possible path of operation reachable by an inverse a-shuffle—from deck to randomly dealt piles to final permutation—appears with probability $1/a^n$.

(ii) **[2]** 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. You do not need to justify.

(iii) **[7]** Show that the transition probability from σ to τ of the inverse a-shuffle is the same as the transition probability $\tau \to \sigma$ of the standard a-shuffle. Refer to the definitions from after problem 4.

Solution to Problem 16:

(a) (i) Clear from earlier calculations.

(ii) Given a deck cut into piles of size $j_1, \ldots, j_a$, there are necessary $\binom{n}{j_1, \ldots, j_a}$ outcomes which must be equally likely. Therefore the probability of getting piles of size $j_1, \ldots, j_a$ must be proportional to $\binom{n}{j_1, \ldots, j_a}$. Or it is just enough to note that probability of each individual path determines the probability for each middle stage of process tree.

(b) It is enough to show that the sequential a-shuffle also satisfies the property of 15(c): every possible permutation occurs with equal probability given the initial cut, as it characterizes the maximum entropy a-shuffle.

Consider the relative location of cards in pile 1 and 2. After shuffling pile 1 and 2 together, order of cards within those piles do not change anymore. So shuffling of pile 1 and 2 together should be uniquely determined if final permutation is given. Similarly we can show that in each 2-shuffles in the sequence should follow certain path to reach the final permutation. Thus the probability for all permutations should be same.

(c) (i) Clear.

(ii) 2413 is unique answer.

(iii) Both for the standard a-shuffle and inverse a-shuffle, we showed that the transition probability of a permutation is the number of possible paths to the permutation divided by a^n. Hence it suffices to show that the path from σ to the set of piles $\mathscr{P}$ to τ exists under the inverse a-shuffle if and only if the path from τ to $\mathscr{P}$ to σ exists under the standard a-shuffle. In an inverse shuffle, the path $(\sigma, \mathscr{P}, \tau)$ is possible if and only if merging $\mathscr{P}$ gives the target permutation τ and the cards in each pile of $\mathscr{P}$ are in order within σ. But in the standard shuffle, the path $(\tau, \mathscr{P}, \sigma)$ is possible if and only if merging $\mathscr{P}$ gives the original permutation τ and the cards in each pile of $\mathscr{P}$ are in order within σ. The two conditions coincide exactly.

17. (a) **[7]** 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) **[15]** 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.

Solution to Problem 17:

(a) Label each card with two numbers according to the piles it landed in during the a-shuffle and the b-shuffle. Those cards with the same label form a pile in an ab-shuffle.

(b) Let $P_a(\sigma \to \tau)$ and $P^a(\sigma \to \tau)$ be the transition probabilities from σ to τ for the standard a-shuffle and inverse a-shuffle respectively. The probability of obtaining τ from σ after an a-shuffle and a b-shuffle is given by

$$\sum_{\mu} P_a(\sigma \to \mu) P_b(\mu \to \tau)$$

where the sum is taken over all permutations μ. Meanwhile problem 16(c) gives $P_a(\sigma \to \mu) = P^a(\mu \to \sigma)$, so this sum is the same as $\sum_\mu P^a(\mu \to \sigma) P^b(\tau \to \mu)$. Now this can be interpreted as the probability of obtaining σ from τ after an inverse b-shuffle and inverse a-shuffle, and according to 17(a) this is the same as $P^{ba}(\tau \to \sigma)$. Applying problem 16(c) again gives $P^{ba}(\tau \to \sigma) = P_{ab}(\sigma \to \tau)$, so we are done.

18. (a) **[7]** Suppose σ is a permutation with r rising sequences. Prove that the transition probability from 1 to σ for GSR a-shuffle of an n-card deck is

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

(b) **[3]** Use this to give another proof of Worpitzky's identity.

(c) **[7]** 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.

Solution to Problem 18:

(a) We need to count the number of different ways to cut the deck into piles which have σ as a possible resulting permutation. We will make $a-1$ cuts which can be in any of $n+1$ locations in the deck. The rising sequences determine $r-1$ of these cuts, but the remaining $a-r$ can be assigned arbitrarily. This gives $\binom{a+n-r}{n}$ ways in which the deck can be cut. There are a^n possible final permutations (counting repeats), giving the desired probability.

(b) Immediate.

(c) The probability is $\binom{a^k+n-r}{n}\frac{1}{a^{kn}}$ where r is the number of rising sequences of σ. This is

$$\left(\frac{a^k+n-r}{a^k}\right)\cdots\left(\frac{a^k+1-r}{a^k}\right)\cdot\frac{1}{n!}$$

and each multiplicative factor can be rewritten as $1+\frac{n-i-r}{a^k}$, which approaches 1 as k approaches ∞. Thus the whole expression approaches $1/n!$.

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 Stanford 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 people, magicians for example, 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. (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 drops the original bottom card first and leaves the original top card on the top, whereas I drops the original bottom card second and leaves the card originally at the top 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 that shuffle to $0, 1, \ldots, 2n-1$ before getting $0, 1, \ldots, 2n-1$ back.

19. Compute (no explanation needed)

    (a) **[2]** $I(O(I(0, 1, 2, 3, 4, 5)))$,

    (b) **[2]** the order of O on 8 cards, and

    (c) **[2]** $O^k(0, 1, 2, 3, 4, 5, 6, 7)$ for all $k \geq 1$.

    Solution to Problem 19:

    (a) $5, 3, 4, 1, 2, 0$

    (b) 3

    (c) $k \equiv 0 \pmod 3 : 0, 1, 2, 3, 4, 5, 6, 7$
    $k \equiv 1 \pmod 3 : 0, 4, 1, 5, 2, 6, 3, 7$
    $k \equiv 2 \pmod 3 : 0, 2, 4, 6, 1, 3, 5, 7$

20. (a) **[3]** Prove that after one out-shuffle of $2n$ cards, the card numbered j has moved to position $2j \pmod{2n-1}$.

    (b) **[3]** Prove that the order of the in-shuffle on $2n$ cards is the same as the order of the out-shuffle on $2n+2$ cards.

    (c) **[2]** Prove that the order of the out-shuffle on $2n$ cards is the least positive integer k such that $2^k \equiv 1 \pmod{2n-1}$.

    (d) **[2]** Compute the order of the out-shuffle on 52 cards.

    Solution to Problem 20:

    (a) For $j \leq n-1$, j moves to $2j$, immediately before $j+n$. That is, $j+n$ moves to $2j+1 = 2(j+n) - (2n-1) \equiv 2(j+n) \pmod{2n-1}$.

    (b) Add a card to the beginning and end; now each in-shuffle is just an out-shuffle with two ghost cards that never move.

    (c) From part a, it is evident that after k out-shuffles, the card numbered j has moved to position $2^k j \pmod{2n-1}$. Thus, the order of the out-shuffle on this deck is the least positive integer k so that $j \equiv 2^k j \pmod{2n-1}$ for all j, i.e. the least positive integer k such that $2^k \equiv 1 \pmod{2n-1}$.

    (d) We have a deck of $52 = 2n$ cards, where $n = 26$ (so $2n - 1 = 51$). Therefore the order of the out-shuffle on this deck is the least positive integer k such that $2^k \equiv 1 \pmod{51}$, and we can quickly check that this integer k is 8.

21. (a) **[3]** Take a deck of 2^m cards and number them as usual. Prove that if a card's number has binary representation $\underline{a_{m-1}a_{m-2}\ldots a_0}$, then after one out-shuffle, that card has moved to position $\underline{a_{m-2}\ldots a_0 a_{m-1}}$.

    (b) **[3]** What do m in-shuffles do to 2^m cards? Justify.

    Solution to Problem 21:

    (a) This follows directly from $j \to 2j \pmod{2^m - 1}$.

(b) Performing m in-shuffles on a deck of 2^m cards will reverse the order of the cards in the deck. We can think of these in-shuffles as out-shuffles on $2^m + 2$ cards, where the top and bottom cards are "dummy" cards that never move. Then, the jth card goes to $2^m j \equiv -j \pmod{2^m + 1}$.

22. **[8]** 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.)

Solution to Problem 22: Interpret 1 as in and 0 as out in the aforementioned binary expansion and perform the resulting operations from left to right. You start with the card numbered 0 and the first in-shuffle takes it to position 1. Note that if your card is at position j, for j not too large, an out-shuffle takes it to $2j$ and an in-shuffle takes it to $2j+1$—so each operation pushes the binary expansion of j to the left and adds the appropriate 0 or 1 in the units digit. This process will never result in a position greater than $2n - 1$, so you need not worry about modding out by $2n - 1$.