Permutation Enumeration

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 $n = 5$.

   Solution to Problem 1:

   (a) $(1, 2, 3)$, $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$, $(3, 2, 1)$
   (b) $n!$, For $n = 5$ there are 120 permutations

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 $\{1, 2, \ldots, n\}$.

   Solution to Problem 2:

   (a) $(2, 1, 3, 6, 5, 4)$
   (b) $(2, 4, 1, 3)$, $(5, 1, 4, 2, 6, 3)$.
   (c) It is enough to show that $\tau^{-1} \circ \sigma^{-1}$ is inverse of $(\sigma \circ \tau)$. It can be proven to be

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

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.

   Solution to Problem 3:

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

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

   Solution to Problem 4: As in Problem 3, the permutation $\mu = \tau \circ \sigma^{-1}$ which changes σ into τ also changes 1 into $\tau \circ \sigma^{-1}$.

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.

   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) $(1, 2, 4, 3)$, $(1, 3, 2, 4)$, $(1, 3, 4, 2)$, $(1, 4, 2, 3)$, $(2, 1, 3, 4)$, $(2, 3, 1, 4)$, $(2, 3, 4, 1)$, $(2, 4, 1, 3)$, $(3, 1, 2, 4)$, $(3, 4, 1, 2)$, $(4, 1, 2, 3)$.

6. 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. 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 $1 \le i \le n$, 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 this 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. This produces $k+1$ permutations of $\{1, 2, \ldots, n\}$ with k ascents.

Combining these two cases yields the desired recurrence.

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

Solution to Problem 8:

n	$\left\langle {n \atop 0} \right\rangle$	$\left\langle {n \atop 1} \right\rangle$	$\left\langle {n \atop 2} \right\rangle$	$\left\langle {n \atop 3} \right\rangle$	$\left\langle {n \atop 4} \right\rangle$	$\left\langle {n \atop 5} \right\rangle$	$\left\langle {n \atop 6} \right\rangle$
0	1						
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. 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.

[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.

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

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

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}.

The Gilbert-Shannon-Reeds shuffle

11. Compute (no explanations required):

    (a) $\binom{7}{3,2,2}$,

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

    (c) $\binom{100}{99,1,0,0,0}$.

    Solution to Problem 11:

    (a) 210

    (b) 2520

    (c) 100

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.

    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) 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}).

    Solution to Problem 13:

    (a) Can be done by quoting binomial theorem. Alternatively, for a set S of n elements, $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$ counts the subsets of S, which is 2^n.

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

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.

Solution to Problem 14:

(a) 4/9

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

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. 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 after problem 3.

Solution to Problem 15:

(a) Similar to Problem 13.a. Possible solutions are quoting the multinomial theorem, explaining the 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 $n!$.)

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.

Solution to Problem 16:

(a) 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 $\binom{n}{j_1,\ldots,j_a}$.

(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 piles 1 and 2 together, the order of the cards within those piles does not change anymore. Thus, the shuffling of piles 1 and 2 together is uniquely determined if the final permutation is given. Similarly, in each of the 2-shuffles in the sequence we must follow a specific path to reach the final permutation. Thus the probability for all permutations should be same.

(c) (i) 2413 is the unique answer.

(ii) For the standard a-shuffle, we showed that the transition probability of a permutation is the number of possible paths to the permutation divided by a^n. It is easy to see that this is also true for the inverse a-shuffle. 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) 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.

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 $P^{ab}(\tau \to \sigma)$. Applying problem 16(c) again gives $P^{ab}(\tau \to \sigma) = P_{ab}(\sigma \to \tau)$, and the proof follows.

18. (a) 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) 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.

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) It is easy to see using a double induction proof that the number of permutations with r rising sequences equals $\left\langle {n \atop r-1} \right\rangle$. Thus, using the symmetry property of of Eulerian numbers, $1 = \frac{1}{a^n}\sum_{r=0}^{n}\left\langle {n \atop r-1} \right\rangle\binom{a+n-r}{n} = \frac{1}{a^n}\sum_{r=0}^{n}\left\langle {n \atop n-r} \right\rangle\binom{a+n-r}{n} = \frac{1}{a^n}\sum_{r=0}^{n}\left\langle {n \atop k} \right\rangle\binom{a+k}{n}$ where $k = n-r$.

(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 $1/n!$.

Perfect shuffles

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 $k \geq 1$.

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) 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 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.

Solution to Problem 20:

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

(b) Add a card to the beginning and end; now each out-shuffle on the $2n+2$ cards is just an in-shuffle on the middle $2n$ cards with two ghost cards at the end that never move.

(c) This follows from part a.

(d) 8

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

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

Solution to Problem 21:

(a) Follows from $j \to 2j \pmod{2^m - 1}$, since the $a_{m-1}2^m \equiv 1 \pmod{2^m - 1}$.

(b) Reverses them. This is clearest from the perspective of an out-shuffle on $2^m + 2$ cards, in which the jth card goes to $2^m j \pmod{2^m + 1}$, or $-j \pmod{2^m + 1}$.

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.)

Solution to Problem 22: Interpret 1 as in and 0 as out in the aforementioned binary expansion (with the left-most digit being 1) and perform the resulting operations from left to right. The number 0 starts out in the 0^{th} position, and the first in-shuffle takes it to the 1^{st} position. 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 you do pushes the binary expansion of j to the left and sticks an appropriate 0 or 1 in the units digit. You never have to mod out because this process doesn't overshoot.