Introduction to Permutations

Let's take a look at a standard 52-card deck of playing cards.

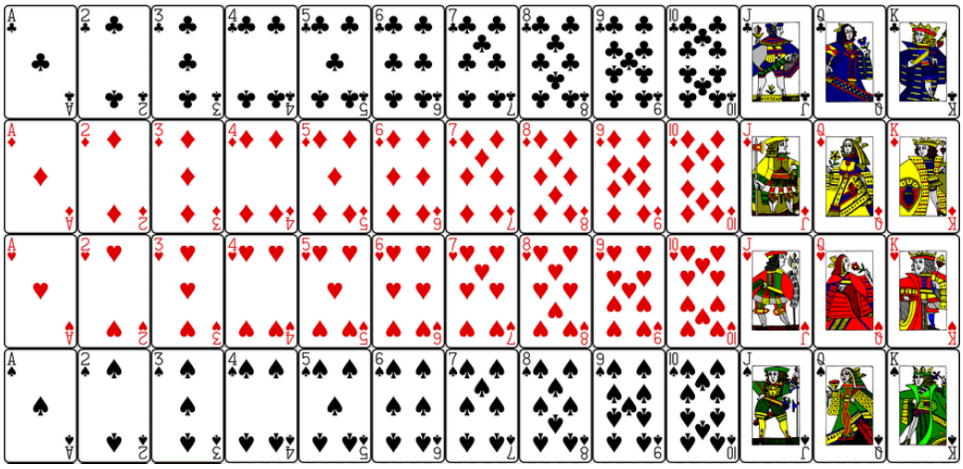


Figure 1: Here we see all 52 cards in a standard deck. The cards are organized into are four separate suits including clubs (♣), diamonds (♦), hearts (♥), and spades (♠). Each suit contains thirteen cards.

In the 52-card deck pictured in Figure 1 above, there are four suits in this deck that come in two separate colors: black is used for spades (♠) and clubs (♣) while red is used for hearts (♥) and diamonds (♦). Each suit has a total of 13 cards including three face cards known as a jack, a queen, and a king that are labeled with the letters "J," "Q," and "K" respectively. Then we have the numeral cards which are labeled from 2 to 10. Finally, each suit has a special ace card that is labeled with the letter "A". During a card game (like poker, blackjack, or cribbage), players shuffle the deck multiple times to rearrange the cards in an unpredictable order. In this lesson, we explore some intriguing questions related to the shuffling process including each of the following:

1. Which quantity is largest?

   A. The number of grains of sand on earth.

   B. The number of stars in the universe.

   C. The number of ways to order a deck of 52 cards.

   D. The number of water molecules in the Earth's oceans.

   E. The number of seconds since the beginning of time.

2. Is there one shuffle to rule them all? In other words, is there one shuffling motion that allows us to generate all possible orderings?

3. What other patterns describe how shuffling works?

To answer to these questions, we study permutations.

What is a permutation?

Permutations are special types of functions used in almost every branch of mathematics. Permutations also show up in other STEM fields. For example, computer scientists rely on permutations to create and analyze sorting algorithms. Quantum physicists deploy permutations in several branches of modern quantum mechanics. Biologists leverage permutations to describe RNA sequences.

In applied linear algebra, we use permutations to construct the determinant function. We also translate permutations into a special class of matrices, known as permutation matrices, which are a subset of the larger family of orthogonal matrices. We employ permutation matrices combined with matrix multiplication to swap rows or columns of a target matrix. In this context, permutations matrices are tools used to solve linear systems problems via computer algorithms. For a preview of coming attractions, search the phrase 'Gaussian Elimination with partial pivoting using permutation matrices'. For now, let's jump into our play with permutations.

We begin our exploration by developing our intuition. One way to think about a single permutation is as a distinct way to arrange a given set of n objects into an ordered sequence, where $n \in \mathbb{N}$ is a positive integer. Another way to say this is that a single permutation is one possible answer to the following question: "how can we put a collection of n objects into a specific order?"

To make this general scenario more concrete, let's conduct a thought experiment. Imagine that a permutation π is a specific way of ordering a set of n balls into a set of n boxes. Before we place balls into boxes, we mark each of the n balls with a unique label chosen from the set $[n] = \{1, 2, 3, ..., n\}$ so that each ball can be named using a positive integer and no two balls are labeled using the same number. We also label each of the n boxes following the same pattern. Mathematically, we say that a permutation is a function $\pi : [n] \to [n]$ that places the individual balls into the individual boxes so that each box contains a single ball. The diagram below illustrates our set up when $n = 6$.

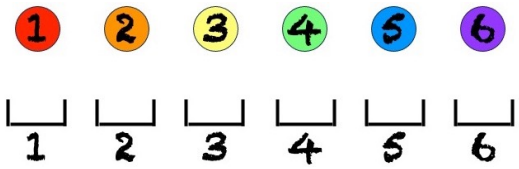


Figure 2: This diagram provides a fun way to visualize the inputs to our permutation function as a set of $n = 6$ balls, each one labeled with a distinct positive integer. The output values of our function are a set of $n = 6$ boxes with similar labels. When we create a permutation, we assign each ball into a corresponding box thus mapping each input value to a single output value.

Later in this lesson, we explore the mathematical definition of a permutation as a special type of function that maps the input set $[n]$ (the labeled balls) into the output set $[n]$ (the labeled boxes).

EXAMPLE 1

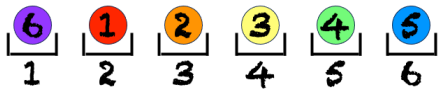
Suppose we start with six balls and six bins, where we label each set with the numbers $1, 2, 3, 4, 5$ and 6. The diagrams below present four possible ways to arrange our balls into a specific order.

$$\pi(1) = 1, \quad \pi(2) = 2, \quad \pi(3) = 3,$$
$$\pi(4) = 4, \quad \pi(5) = 5, \quad \pi(6) = 6.$$

Figure 3: One way to order our set of $n = 6$ objects is to maintain the natural numeric order by simply mapping ball k to box k for $k \in [6]$. In function notation, we write the ball number as the input to our function. The number on the box in which each ball gets place is the output to our function. If we name our permutation π, then we can write $\pi(1) = 1$ to represent that ball 1 gets placed into box 1.

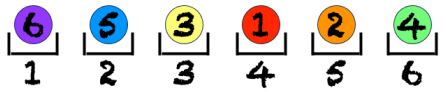
$$\sigma(1) = 2, \quad \sigma(2) = 1, \quad \sigma(3) = 4,$$
$$\sigma(4) = 3, \quad \sigma(5) = 6, \quad \sigma(6) = 5.$$

Figure 4: Another option we can use to order our balls is to do swaps in pairs of two. In this case we see that we swap balls 1 and 2, balls 3 and 4, and balls 5 and 6. If we call this permutation σ, then we can write $\sigma(1) = 2$ and $\sigma(2) = 1$ to represent that fact that we put ball 1 in box 2 and ball 2 in box 1.



$$\tau(1) = 6, \quad \tau(2) = 1, \quad \tau(3) = 2,$$
$$\tau(4) = 3, \quad \tau(5) = 4, \quad \tau(6) = 5.$$

Figure 5: In this case, we push and pop. We push each of the balls one to the right and pop that last ball back to the first box. To write this specific rule for ordering our balls using function notation, wenamel this permutation τ.



$$\beta(1) = 6, \quad \beta(2) = 5, \quad \beta(3) = 3,$$
$$\beta(4) = 1, \quad \beta(5) = 2, \quad \beta(6) = 4.$$

Figure 6: Let's get our fancy pants on and create an order that takes a little more effort to describe verbally. We name this permutation β to describe the way we put the balls in order.

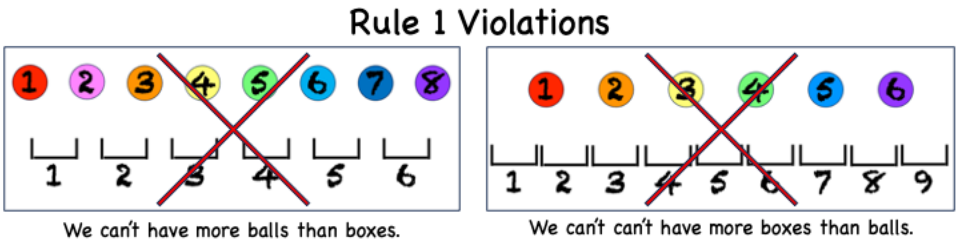
Each of these four permutations represents one possible way to put a set of 6 balls into a specific order. Remember that in our introduction to this lesson, we asked some interesting questions about how many ways there are to shuffle a 52-card deck. In that case, we can think about each shuffle as one possible way to put 52 balls into 52 boxes. Here we study a smaller case as an introduction to the larger problem.

What does not qualify as a permutation?

Before we develop a technical mathematical definition, let's delineate a clear list of rules for our play with permutations. We do this be creating a concrete list of four rules for how we define permutations.

Rule 1: The finite number of balls must be equal to the number of boxes.

Another way to state rule 1 for our study of permutations is that we are not allowed to have more balls than there are boxes nor are we allowed to have more boxes than there are balls.

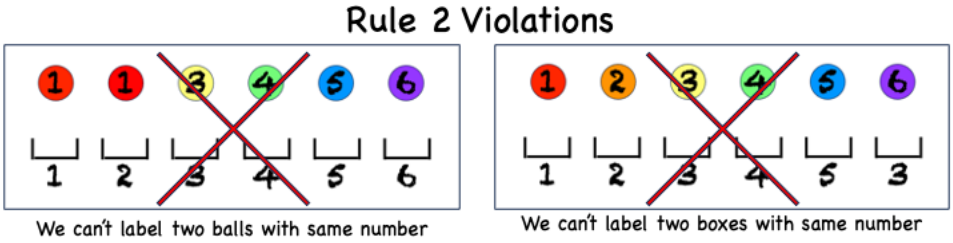


We can also have a lot of fun with exploring what happens if we map a set of n balls into a set of x boxes where we don't require that $n = x$ for $n, x \in \mathbb{N}$. However, that is not the game we play when we study permutations. Instead, we say that for a permutation, the number of balls must be exactly equal to the number of boxes.

We can formalize rule 1 in the language of functions by saying that a permutation π is a special type of function in which the the domain space is equal to the codomain with $\pi \subset [n] \times [n]$.

Rule 2: The n balls and n boxes must be labeled with distinct positive integers

The second rule that we impose is that we must be able to distinguish between each ball and each box. We violate this rule if we label two of the balls using the same number or if we label two of the boxes with the same number.



Rule 2 is equivalent to saying that the input balls and output boxes are distinct objects that we can tell apart from each other.

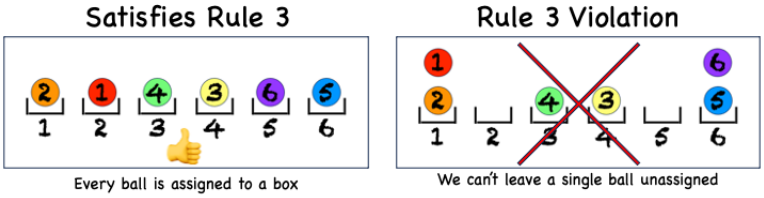
Rule 3: We must assign all balls to a box (i.e. we can't leave a ball unassigned).

Our third rule requires that we place every ball inside a box. Mathematically, this rule is equivalent to the first part of our set theoretic definition of a function from our Lesson on Relations and Functions. Recall that we say that a relation $\pi \subset [n] \times [n]$ is a function from $[n]$ to $[n]$ if two conditions are satisfied:

i. The domain of π is equal to the domain space.

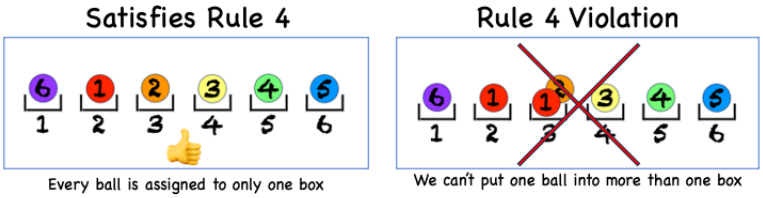
ii. If $(k, x) \in \pi$ and $(k, z) \in \pi$, then $x = z$.

Rule 3 puts into words the condition that $\text{Dom}(\pi) = [n]$ since we are requiring that any permutation π actually assign every input value in the domain space $[n]$ to some output value in the range.



Rule 4: Each ball can only be placed into a single box.

Our fourth rule suggests that the balls do not exist in the quantum realm. In other words, no ball can be mapped into two different boxes at the same time. This rule is equivalent to requiring that our permutation "pass the vertical line test" so that every one input gets map to a single output. We might also say that this rule requires that each input is monogamous. Using mathematical notation we say that permutations $\pi : [n] \to [n]$ satisfy the second condition of being a function so that if $\pi(k) = x$ and $\pi(k) = z$, then $x = z$.



Rule 4 combined with rules 1 and 3 imply that every box gets at least one ball which is equivalent to stating that $Rng(\pi) = [n]$. These rules guarantee that a permutation $\pi : [n] \to [n]$ is an injective and surjective function.

How do we formally define permutations?

Let's transform the rules of our game into a formal definition.

Definition 1: Permutation

Let $[n] = \{1, 2, 3, ..., n\}$ be the set of the first n positive integers. A **permutation** of [n] is a bijective function from $[n]$ to itself. In other words, a permutation is a map $\pi : [n] \longrightarrow [n]$ such that

i. π is one-to-one: if $\pi(i) = \pi(k)$, then $i = k$

ii. π is onto: $\text{Codomain}(\pi) = \text{Rng}(\pi) = [n]$

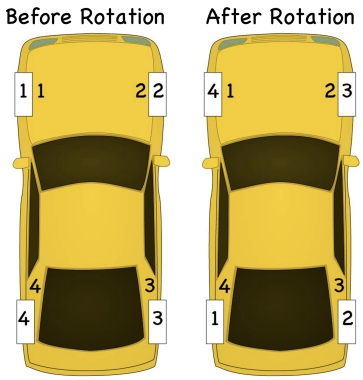
The condition that any permutation π is one-to-one, also known as *injective*, is equivalent to stating that each box can contain only one ball so that each input is mapped to a unique output. On the other hand, the requirement that any permutation π is onto, also known as *surjective*, is equivalent to stating that each box must contain at least one ball. We say that a function is *bijective* if it is both injective and surjective. Since the number of boxes equals the number of balls, we see that any permutation π is a map that assigns n balls into n boxes with each box containing only one ball.

EXAMPLE 2

Imagine you want to rotate the tires on your car during a routine visit to your local mechanic. At the beginning of the job, each of the four tires is located on your car in one of the four positions. To label each tire and each wheel well using the set $[4] = \{1, 2, 3, 4\}$, you sit in the drivers seat, and label the front left tire with the number 1, the front right number 2, the back right tire number 3 and the back left tire number 4. To rotate your tires, you want to place each tire in one of the four positions on the car and no two tires can be placed in the same location. One possible rearrangement is given by map σ:

$$\sigma(1) = 4, \qquad \sigma(2) = 3, \qquad \sigma(3) = 2, \qquad \sigma(4) = 1.$$

In the figure below, we can visualize this change:



This permutation implies that we keep the tires on the same side of the car while swap the front and back tires. Our mapping σ is injective since each $i \in [4]$ has a unique image under σ. We see that f is surjective since $\text{Rng}(\sigma) = [4]$. In other words the map σ that your mechanic uses to rotate your tires satisfies our definition of a permutation.

Permutations are so powerful and ubiquitous that we will find it useful to give the set of permutations a special name.

Definition 2: S_n is the set of all permutations of n elements

Let $[n] = \{j \in \mathbb{N} : 1 \leq j \leq n\}$. The set of all permutations on $[n]$ is denoted as S_n. These are exactly the set of one-to-one maps from the set $[n] = \{1, 2, ..., n\}$ to itself.

What notation can we use to describe permutations?

Many mathematical authors use lowercase Greek letters to denote permutations. In popular mathematics textbooks, permutations are commonly written using any of the greek letters written below.

Greek letter	English translation
α	alpha
β	beta
σ	sigma
τ	tau
π	pi

Remember that permutations are functions that act on multiple input objects. To describe these functions, we can use many different types of notation. In our tire rotation example above, we defined a special permutation in S_4 using *piecewise function notation* in the form

$$\sigma(1) = 4, \qquad \sigma(2) = 3, \qquad \sigma(3) = 2, \qquad \sigma(4) = 1.$$

This can also be called *function notation*. When we define a permutation using piecewise function notation, we specify the action of each permutation using an elementwise definition so that we explicitly identify the input-output action that the permutation has on each individual input value inside $[n]$. A similar approach can be achieved by using *arrow notation* to map each input to its corresponding output value via a small arrow. For our tire rotation example, we have

$$1 \mapsto 4 \qquad 2 \mapsto 3 \qquad 3 \mapsto 2 \qquad 4 \mapsto 1.$$

When we use either function or arrow notation to define a permutation, we must explicitly identify the action of the permutation on each input value so that we write n versions of the following type of statement:

$$\underbrace{\pi(i) = k}_{\text{function notation}} \qquad \text{or} \qquad \underbrace{i \mapsto k}_{\text{arrow notation}}$$

for some $i, k \in [n]$.

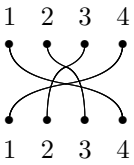
Defining permutations using either function and arrow notation can be quite tedious. To alleviate some of the monotony involved in making these types of definitions, we might use several other types of notation. One very popular approach is *Cauchy's two-line notation* for a permutation $\pi : [n] \longrightarrow [n]$, which is a compact and convenient way to define the permutation where we write:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}.$$

We place the ordered list of the input elements of $\pi \in S_n$ in the first line of our two line notation. Directly below each input element, we place its image under the map π. We organize these outputs into the second row directly below the first row in our two line notation. Using this set up, we can easily see that the image of i is $\pi(i)$ under the map π. Going back to the tire rotation example, we have

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

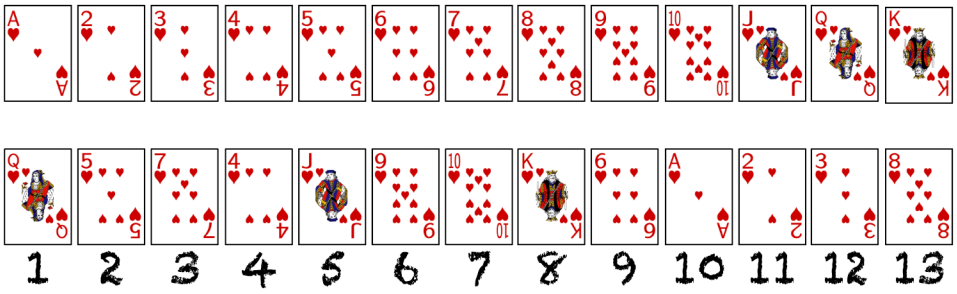
Later in this lesson, we explore a composition operation to combine multiple permutations together. We use permutation composition to generate new permutations from a given set of permutations or to decompose a complex permutation into a composition of simpler permutations. When studying the composition operation, we can visualize the action of each permutation using a using a *permutation diagram*. Below is an example of a permutation diagram for our tire rotation example.



To create this permutation diagram, we draw two rows of n dots and label these dots, in order from left to right, with the numbers from the set $[n] = \{1, 2, 3, ..., n\}$. We think about the upper row of dots as the inputs and the lower row as the outputs. Then we draw connection lines or curves from each input dot to its corresponding output as defined by the permutation.

EXAMPLE 3

Every shuffle of a deck of cards is a rearrangement of the order of the deck. We might think of each shuffle as a permutation. To illustrate this idea, let's create an example where we shuffle the 13 heart cards in a standard 52-card deck.



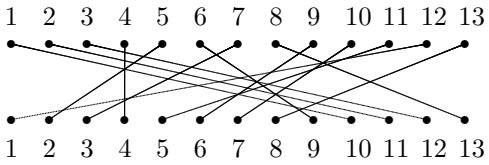
Let's number our 13 heart cards by counting with the ace of hearts as the number 1, the 2 of hearts as the number 2, the 3 of hearts as the number 3, and so on. In our count, we assume a standard ordering convention that the Jack of hearts comes after the 10 of hearts and is counted as the number 11. After the Jack comes the Queen which we enumerate with the number 12. We end our count with the King of hearts which is labeled with the number 13. Given our diagram above, we define the permutation that corresponds to this particular shuffle. Let's first define this permutation $\tau : [13] \to [13]$ using function notation:

$$\begin{aligned} &\tau(1) = 10, \quad \tau(2) = 11, \quad \tau(3) = 12, \quad \tau(4) = 4, \quad \tau(5) = 2, \\ &\tau(6) = 9, \quad \tau(7) = 3, \quad \tau(8) = 13, \quad \tau(9) = 6, \quad \tau(10) = 7, \\ &\tau(11) = 5, \quad \tau(12) = 1, \quad \tau(13) = 8. \end{aligned}$$

While this use of function notation accurately describes the shuffle, it's also a bit cumbersome. Alternatively, we can define this permutation using Cauchy's two line notation:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 10 & 11 & 12 & 4 & 2 & 9 & 3 & 13 & 6 & 7 & 5 & 1 & 8 \end{pmatrix}.$$

We can also draw our permutation diagram for this shuffling action.



Any of these definitions provide a complete and accurate description of the action of the shuffle.

How many permutations of n elements are there?

We now understand what a permutation is and we can use various notational conventions to define a permutation. The next step in our study is to find patterns that might help us better understand how permutations work so that we might use these interesting maps to solve problems that we care about.

We begin this process by counting the total number of permutations in the set S_n for any $n \in \mathbb{N}$. Another way to ask this question is: how many possible ways can we order n items? We can also ask: how many different ways can we arrange n objects into n different places? We begin our study of these questions by exploring the first few examples with $n = 1, 2, 3, 4$. The goal of studying these base cases is to identify patterns. Then we generalize our observations to come up with a conjecture for any value of $n \in \mathbb{N}$. Then we generate a proof for our conjecture and we call this a theorem.

EXAMPLE 4

We start with the least interesting case and analyze all the permutations in the set S_1. This is the set of all different arrangements of one element. By our definition of S_1, we want to find all bijective maps

$$\pi : \{1\} \longrightarrow \{1\}$$

The first question we ask is: how many different options do we have for the output of any permutation on the first input element 1. The set [1] contains a single element, there is only one possible way to map this set onto itself:

$$\pi_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

In other words, the set S_1 has exactly one element.

EXAMPLE 5

Let's list all the permutations in S_2. By our definition of S_2, we want to find all bijective maps

$$\pi : \{1, 2\} \longrightarrow \{1, 2\}.$$

We start with the question: how many different boxes can we send our first ball into? For S_2 we see that $n = 2$ so we have two balls and two boxes. We can put ball number 1 into one of two bins. Either we put ball 1 into box 1 or we place ball 1 into box 2. This is a total of two choices for our placement of the first ball. Once we place ball number 1 into either of these two choices, there is only one choice remaining for the location of ball 2. If we place ball 1 into box 1, then ball 2 must

be placed into box 2. Conversely, if we place ball 1 into box 2, then ball 2 must end up in box 1. Since we have 2 choices for the placement of ball 1 and in each of those cases we have only 1 choice for the placement of ball two, we have a total of $2 \cdot 1 = 2! = 2$ different permutations in the set S_2. We list these below:

$$\pi_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \qquad \pi_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

EXAMPLE 6

Consider S_3, the set of all ways to order three elements. Once again, we ask ourselves the question: if we have three balls and three boxes, how many ways can we place the balls into the boxes. To figure this out, we begin by placing ball number 1 and notice that we have a total of 3 different choices. We can place ball 1 into box 1, 2, or 3. Once we place ball number 1 into one of the boxes, then it's time to place ball number 2. However, since one of the boxes already contains ball 1, we have only 2 choices for the placement of the second ball: placing ball 1 leave one less choice for the second ball. After we place ball 2, our final task is to put ball 3 into a box. But, since two of the three boxes already have balls inside, we have a unique choice for ball three. Thus, we have a total of $3 \cdot 2 \cdot 1 = 3! = 6$ different options. We provide the complete list of the six unique permutations in S_3 below:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

EXAMPLE 7

The set S_4 contains all permutations of the first four positive integers. To count of the number of elements in S_4, we ask ourselves: how many different ways can we place four balls, labeled with the numbers 1 to 4, into four boxes which are similarly labeled? For the first ball, we have one of four choices: we can place ball one into box 1, 2, 3, or 4. Once ball one is placed, this leaves a total of three open boxes for the placement of ball 2. Continuing in this manner, we conclude that there are a total of $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$ different ways to put our 4 balls into our 4 boxes. Let's confirm this intuition by listing every permutations in S_4:

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}}_{\pi_1} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}}_{\pi_2} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}}_{\pi_3} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}}_{\pi_4}$$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}}_{\pi_5} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}}_{\pi_6} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}}_{\pi_7} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}}_{\pi_8}$$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}}_{\pi_9} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}}_{\pi_{10}} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}}_{\pi_{11}} \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}}_{\pi_{12}}$$

$$\underbrace{\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}}_{\pi_{13}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}}_{\pi_{14}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}}_{\pi_{15}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}}_{\pi_{16}}$$

$$\underbrace{\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}}_{\pi_{17}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}}_{\pi_{18}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}}_{\pi_{19}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}}_{\pi_{20}}$$

$$\underbrace{\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}}_{\pi_{21}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}}_{\pi_{22}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}}_{\pi_{23}} \quad \underbrace{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}}_{\pi_{24}}$$

Let's review our first few cases and look for a pattern. To do this, we rely on some useful notation. We say that the symbols $|S_n|$, read as *the cardinality of* S_n, represent the number of elements in S_n for any $n \in \mathbb{N}$. Using this notation, we create the table below.

n	$\lvert S_n \rvert$
1	$1! = 1$
2	$2! = 2 \cdot 1 = 2$
3	$3! = 3 \cdot 2 \cdot 1 = 6$
4	$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$

We use this table to identify a pattern that we can extend to make guesses about larger values of n. For example, we might ask ourselves: what is $|S_5|$ or $|S_6|$? How about $|S_{13}|$? Based on the first four cases, we might guess the answers to these questions to be

$$|S_5| = 5! = 120, \qquad |S_6| = 6! = 720, \qquad \text{and} \qquad |S_{13}| = 13! = 6227020800.$$

We might make a more far reaching conjecture that $|S_n| = n!$. To transform this conjecture into a theorem, we need only produce a proof. In our work enumerating every element in S_1, S_2, S_3 and S_4, we outline one possible approach to counting the number of elements in S_n for any $n \in \mathbb{N}$.

Theorem 1: The Number of Elements of S_n

Let $[n] = \{1, 2, ..., n\}$. If S_n is the set of all bijections from $[n]$ to $[n]$, then there are a total of $n! = n \cdot (n-1) \cdots 2 \cdot 1$ elements of S_n.

Proof. Let $\pi : [n] \to [n]$ be a permutation. To assign our first element 1 in our domain, we can choose any of n elements in the codomain leaving a total of n choices. After we have assigned the output value of $\pi(1)$, we move onto choosing an output $\pi(2)$. We have a total of $(n-1)$ possible choices since our permutation must be one-to-one and we have already assigned one output for $\pi(1)$. We continue in this way and notice that each time we assign a new output element, we decrease the

possible number of choices by one. Thus, we see that the total number of possible maps in S_n is given by

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$$

This is what we wanted to show. □

This is our first breath-taking result so far in our exploration of permutations: the number of permutations is counted using the factorial function $n!$. In other words, the size of S_n grows very large (faster than an exponential function) for relatively small values of n. Let's look at $|S_n|$ for some interesting cases related to our lived experiences:

- There are $4! = 24$ different ways to rotate the tires on a $4-$wheel car.
- For a van with 8 seats and all 8 passengers who can drive, there are $8! = 40320$ different ways to order the passengers in the seats of that van.
- The total number of different shuffles of a 52 card deck is given by 52! which is exactly equal to the following number:

  80658175170943878571660636856403766975289505440883277824000000000000

If you take the time to count the number of digits in 52!, you'll notice there are 68 digits in this number with $|S_{52}| > 8 * 10^{67}$. This is the number of different ways to order a deck of cards. Let's combine this theorem about the number of elements of S_n with some estimations from science to solve our first mystery. Below we present some estimates from various scientific fields for each of the following values:

A. The number of grains of sand on earth $\approx 1 \times 10^{26}$
B. The number of stars in the universe $\approx 1 \times 10^{24}$
C. The number of seconds since the big bang $\approx 436117076600000000 \approx 4 \times 10^{17}$
D. The number of possible configurations of a deck of fifty-two cards $= 52!$
E. The total number of water molecules on Earth $\approx 4.62924 \times 10^{49}$

Think about this for a minute. As of this writing, the human population on earth is around 8 billion people. Let's pretend that every single one of these people shuffled a deck of cards once per second since the beginning of time. Then, the total number of shuffles made would be bounded above by:

$$8 \times 10^9 \cdot 5 \times 10^{17} = 40 \times 10^{26} = 4 \times 10^{27}.$$

This is still a tiny fraction of all of the $52! \approx 8 \times 10^{67}$ possible shuffle arrangements. Another way to say this is that each time you shuffle a deck of cards, it is highly likely that you are the first person ever in the history of this planet to achieve the resulting card ordering.

Using the structure of permutations, we figured out how many possible ways we can shuffle a deck of cards. We also learned a more general skill of counting the total number of permutations of the set $[n]$. Let's deepen our exploration and work to answer our second question where we wonder if there are certain shuffling movements that rule them all? In mathematical terms, we might ask if there is a smaller subset of permutations that, when combined together, can generate any other permutation?

What does it mean to combine permutations together?

Remember that every element $\pi \in S_n$ is a bijective function $\pi : [n] \longrightarrow [n]$ so that the individual elements in S_n are bijective functions. Let's use this realization to reframe our second question using more general language: What does it mean to combine functions together? What operation(s) have we seen that allows us to combine two functions to create a new function?

One option we might choose is the composition of functions. If we start with $\sigma, \pi \in S_n$ and we want to combine these together to make a new permutation $\tau \in S_n$, we might state that

$$\tau = \sigma \circ \pi$$

where the $\circ$ operation is function composition. We might recall from our study of Precalculus and Calculus that we have some special rules for function composition. If we choose a specific element $k \in [n]$, then we say that

$$\tau(k) = (\sigma \circ \pi)(k) = \sigma(\pi(k))$$

In this notation we apply rightmost permutation to the input value k first and then we apply the leftmost permutation second. This approach to the composition of functions $\sigma \circ \pi$ implies that we need to read function compositions from right to left rather than from left to right.

EXAMPLE 8

Let's combine two permutations in S_4 using the composition operation. From our numbering system for elements in S_4 in Example 6 from this section, we have

$$\pi_{18} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \qquad \text{and} \qquad \pi_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

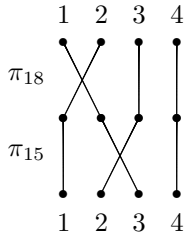
We generate a new permutation by setting $\tau = \pi_{15} \circ \pi_{18}$ and find the output for each element in the input set $[4]$:

$$\begin{aligned} \tau(1) &= (\pi_{15} \circ \pi_{18})(1) = \pi_{15}(\pi_{18}(1)) = \pi_{15}(2) = 3 \\ \tau(2) &= (\pi_{15} \circ \pi_{18})(2) = \pi_{15}(\pi_{18}(2)) = \pi_{15}(1) = 1 \\ \tau(3) &= (\pi_{15} \circ \pi_{18})(3) = \pi_{15}(\pi_{18}(3)) = \pi_{15}(3) = 2 \\ \tau(4) &= (\pi_{15} \circ \pi_{18})(4) = \pi_{15}(\pi_{18}(4)) = \pi_{15}(4) = 4 \end{aligned}$$

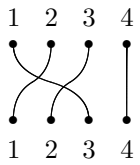
We can write this resulting permutation using two line notation as

$$\tau = \pi_{15} \circ \pi_{18} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

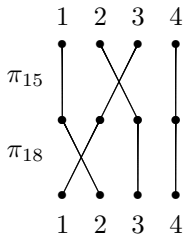
It's worth noting that we already have a name for this permutation in Example 6 with $\tau = \pi_9 \in S_4$. Another way to map the action of the composition $\tau = \pi_{15} \circ \pi_{18}$ is by using a two-level permutation diagram, as seen below:



Notice in this diagram that we first map the action of the rightmost permutation π_{18} followed by the leftmost permutation π_{15}. If we trace the action of the two permutations through the two levels of this diagram, we arrive at the composition permutation. This is identical to the action seen using function notation and results in the following permutation diagram:



It is worth noting that order matters in the composition operation. Sometimes, reversing the order of a composition produces a different permutation. In this example, we see that $\pi_{15} \circ \pi_{18} \neq \pi_{18} \circ \pi_{15}$. We confirm this statement by drawing a permutation diagram to map the action of $\pi_{18} \circ \pi_{15}$:



We notice that under this map we have

$$\pi_{18} \circ \pi_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \pi_{15} \circ \pi_{18}$$

We can sum up this last observation using mathematical terminology by saying that "in some cases, the composition operation is *noncommutative*."

As seen in our example above, the composition of two permutations is another permutation. Each permutation is a bijective map from $[n]$ to itself so the composition must also be a bijection with the same domain and range. Given this nice property, we can define a "product" between elements of S_n.

Definition 3: The product of permutations

Let $n \in \mathbb{N}$. The product of the permutations $\sigma, \pi \in S_n$ is the composition of these functions so that

$$\underbrace{\sigma \cdot \pi}_{\text{product notation}} = \underbrace{\sigma \circ \pi}_{\text{composition notation}}$$

For the action of $\sigma \cdot \pi$ on an element $k \in [n]$, we adopt the convention that the rightmost permutation acts first with $(\sigma \circ \pi)(k) = \sigma(\pi(k))$.

How does the composition operations enhance our notation?

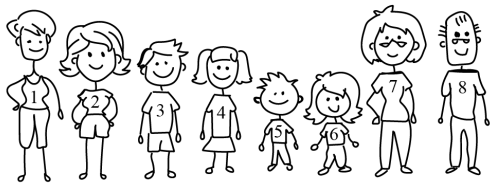
As we saw in Example 7 above, we can use the composition of two permutations in S_n to produce a new permutation in S_n. In the language of cards, we can create

new shuffles from old shuffles. This leads to the intriguing questions: what is the minimum number of shuffling movements that generate all possible orderings of a deck of cards? Is there is one shuffle to rule them all?

To dive deeper into these questions, let's study a subset of permutations known as cycles. A cycle permutation, also known as a cycle, is a special element type in S_n that maps a string of integers with a fixed length cyclically while leaving all other elements unchanged. Let's take a look at some examples to identify what cycles are and how they work.

EXAMPLE 9

Imagine that a family of eight takes a long road trip together in a minivan that seats eight passengers. In this scenario, we have two moms, four kids, and one set of abuelitos (grandparents). In order to assign seats, the family members count off using the numbers $1, 2, 3, ..., 8$ and also label each seat in the car with the same numbers. This humanizes our process of thinking about permutations: instead of assigning balls into boxes, we now think of assigning people to seats. Below we see a diagram of the main idea for this application of permutations.



We begin the road trip using the identity permutation $\pi_1 = 1 \in S_8$ where each family member is assigned to the seat corresponding with their individual number. In Cauchy's two line notation, we write:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

A *cycle permutation*, also known as a *cycle*, is a way to rearranges this original seating order so that a subset of our family members cyclically rotate seats while the position of the other family members remain fixed. The *length of a cycle permutation* is the number of people who move their seats.

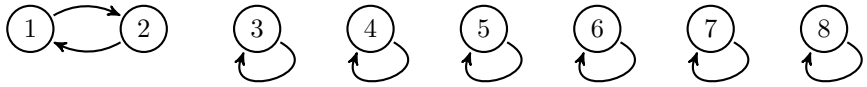
For example, suppose that mom number 1 gets tired of driving. They pull over the car and the two moms swap seats: mom number 2 takes over driving while mom 1 moves into the passenger seat. All other passengers in this arrangement stick to their original position. Since only two members of the family are switching seats, this cycle has length 2 and we call this a $2-$cycle. We define this swap as

permutation $\sigma \in S_8$ with

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

Cauchy's two line notation is helpful in illustrating the permutation's effect on each individual input element. However, two line notation is not designed to highlight the action of each cycle. Because cycles are so powerful in the study of permutations, it can be handy to develop special *cycle notation* to capture the effects of each cycle permutation. This notation comes in two flavors, complete cycle notation and compact cycle notation, which we study below.

The main idea behind cycle notation is to explicitly identify which elements are changed by the cycle as well as each element whose position is fixed. To develop our intuition for cycle notation, let's illustrate the action of our example of the 2−cycle $\sigma \in S_8$ on the individual elements using a diagram, as seen below.



In this diagram, we draw arrows to indicate exactly what the 2−cycle does to each individual element. As shown by our arrows, people 1 and 2 swap positions in the car. All other family members stay seated, which we draw as self loops to represent the idea that our map sends those elements back to themselves.

Although this diagram clearly illustrates the effects of σ on each element of $[n]$, it can be cumbersome to draw nodes, arrows, and labels every time we want to study cycle permutations. This is where our two types of cycle notation come in. The main idea behind the *complete cycle notation* is to demonstrate what a given permutation does to each individual element of $[n]$ by presenting the permutation as a collection of cycles. In complete cycle notation, we list every cycle, including all 1−cycles, to define the permutation completely. We define a *1-cycle* as a cycle that has length one which arises when a permutation fixes an element in $[n]$ (i.e. sends that element back to itself).

We may sometimes find it useful to omit the 1-cycles. To define a permutation using compact cycle notation, we take our complete cycle notation and delete all 1−cycles from our representation. Let's write our 2−cycle σ using these conventions:

$$\sigma = \underbrace{(1\ 2)(3)(4)(5)(6)(7)(8)}_{\text{complete cycle notation}} = \underbrace{(1\ 2)}_{\text{compact cycle notation}}$$

Compare the symbols in the cycle notation with the cycle diagram for σ above. In cycle notation, we use parenthesis and spaces (not commas) to identify exactly what is happening to each element via the action of σ. The notation $(1\ 2)$ represents that 1 gets mapped to 2 and 2 gets mapped back to 1. When we write (3), we mean that element 3 gets mapped to itself under permutation σ (this corresponds to a self loop in our diagram). We notice that $4, 5, 6, 7$ and 8 are also represented in 1−cycles in the complete cycle notation. To create the compact cycle notation, we simply erase all 1−cycles from the representation.

Let's get some more practice with cycle notation by considering other ways our family might want to switch seating positions during the road trip. For example, suppose that brother 3 and sister 4 are fighting while abuelito (grandpa) is feeling a bit stuffy in the back. To fix this problem, the mom in position 2 takes the seat in

position 4, sister 4 takes the seating position 8, abuelito moves up to seat number 2 in front, and all other family members remain seated. Since only three people interchange their seats, we say this is a $3-$cycle $\tau \in S_8$. We represent this action in Cauchy two line notation as

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 8 & 5 & 6 & 7 & 2 \end{pmatrix}$$

Again, we draw a diagram to represent the action of this cycle permutation

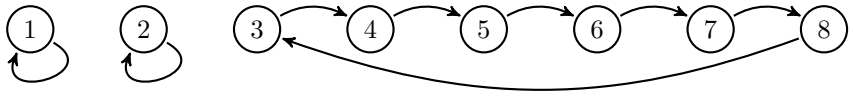
We then translate this diagram into our cycle notation and write

$$\tau = \underbrace{(1)(2\ 4\ 8)(3)(5)(6)(7)}_{\text{complete cycle notation}} = \underbrace{(2\ 4\ 8)}_{\text{compact cycle notation}}$$

To end this example, let's look at one last method our family might use to rearrange their seating order during the trip. In this case, we'll say that everyone that is not sitting in the front of the car will move one seat to the right (moving from seat k to seat $k+1$) while the person in position 8 will move to the seat vacated by the person sitting in seat 3. The two people sitting in the front (the driver in position 1 and the person riding shotgun) remain seated. This is a $6-$cycle permutation $\alpha \in S_8$ defined as

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 5 & 6 & 7 & 8 & 3 \end{pmatrix}$$

We draw a diagram to accurately describe this action.



We then translate this diagram into our cycle notation and write

$$\alpha = \underbrace{(1)(2)(3\ 4\ 5\ 6\ 7\ 8)}_{\text{complete cycle notation}} = \underbrace{(3\ 4\ 5\ 6\ 7\ 8)}_{\text{compact cycle notation}} .$$

Given our examples above, we might think more generally about a $k-$cycle as any permutation that maps a set of k integers cyclically so that the first integer gets mapped to the second one which gets mapped to the third one and so on all the way to the last element which gets mapped back to the first. The other $n-k$ elements remain unchanged (i.e. get mapped back to themselves). Let's write this as a formal definition for future reference.

Definition 4: Cycle permutation of length k

Let $n \in \mathbb{N}$ and suppose $k \in [n]$. Suppose we have k distinct integers $\{m_1, m_2, ..., m_k\} \subseteq [n]$ where $m_i \neq m_j$ for any $1 \leq i \neq j \leq k$. We say that $\sigma \in S_n$ is a *cycle permutation of length k*, also known as a *k-cycle* if

$$\sigma = (\ m_1 \ \ m_2 \ \ m_3 \ \cdots \ m_{k-1} \ \ m_k \ )$$

in compact cycle notation, where σ maps m_1 to m_2, m_2 to m_3, ..., m_{k-1} to m_k, and m_k back to m_1 while all other elements of $[n]$ that are not in the set $\{m_i\}_{i=1}^{k}$ remain fixed (i.e. get sent back to themselves).

Not all permutations in S_n are categorized as cycles. For example, let's look back at the permutation $\pi_{10} \in S_4$ from Example 6 above:

$$\pi_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Based on our definition 4 above, π_{10} is not a cycle permutation since it cannot be written as a single $k-$cycle. Instead, π_{10} is the composition of two different $2-$cycles. To see why this is true, let's remember the permutations $\pi_{13}, \pi_{18} \in S_4$ from Example 6. We write these permutations using cycle notation as

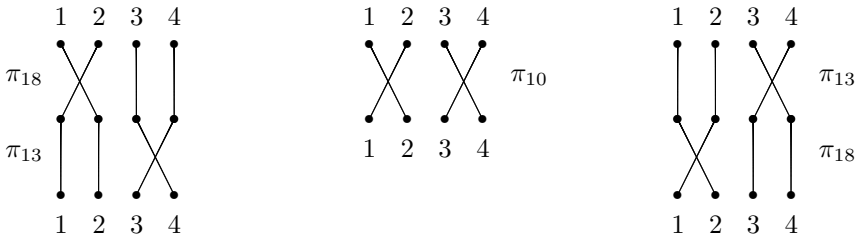
$$\pi_{18} = \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}}_{\text{Cauchy two-line notation}} = \underbrace{(\ 1 \ \ 2 \ ) \, (\ 3 \ ) \, (\ 4 \ )}_{\text{Complete cycle notation}} = \underbrace{(\ 1 \ \ 2 \ )}_{\text{Compact cycle notation}}$$

$$\pi_{13} = \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}}_{\text{Cauchy two-line notation}} = \underbrace{(\ 1 \ ) \, (\ 2 \ ) \, (\ 3 \ \ 4 \ )}_{\text{Complete cycle notation}} = \underbrace{(\ 3 \ \ 4 \ )}_{\text{Compact cycle notation}}$$

If we combine our cycle notation with the composition operation, we can write

$$\pi_{10} = \underbrace{\pi_{13} \circ \pi_{18}}_{\text{Composition notation}} = \underbrace{\pi_{13} \cdot \pi_{18}}_{\text{Product notation}} = \underbrace{(\ 3 \ \ 4 \ ) \cdot (\ 1 \ \ 2 \ )}_{\text{Compact cycle notation}} = (\ 3 \ \ 4 \ ) \circ (\ 1 \ \ 2 \ )$$

It is worth reiterating that we apply our composition operation from right to left so that, if we write $\pi_{10} = \pi_{13} \cdot \pi_{18}$, then the action of π_{18} happens first followed by the action of π_{13} afterwards. To get a concrete idea of what happens when we compose these permutations, let's draw a permutation diagram and then map each element to its image through the multiple steps of the product, as seen below.



An interesting feature of this specific example is that the order of the product doesn't matter. In other words, if we switch the order of the composition in this

special case, we still achieve the same output so that $\pi_{10} = \pi_{13} \cdot \pi_{18} = \pi_{18} \cdot \pi_{13}$. Earlier in this section we noted that in some cases, the composition operation is *noncommutative* meaning that we cannot always switch the order of the composition and maintain equality. However, in our discussion of the permutation $\pi_{10} \in S_4$ above, we see that sometimes we can switch the order of the composition of permutations. In fact, there is a subset of special elements of S_n that do commute via the product of permutations.

Definition 5: Disjoint cycles

Let $n \in \mathbb{N}$. Two or more cycles in S_n are disjoint if they have no numbers in common when written in their compact cycle notation.

One powerful feature of this definition of disjoint cycles is that we can use it as inspiration to discover a unique cycle representation for every single element of S_n. In our example above, we have

$$\pi_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \underbrace{(\ 3\ \ 4\ ) \cdot (\ 1\ \ 2\ )}_{\text{Compact cycle notation}}$$

Notice that even though the original permutation is not a cycle permutation, we can still write π_{10} as a composition of two different $2-$cycles. This general trend holds true for every single element of S_n: we can decompose each element in S_n into the products of disjoint cycles. To do this, we use a *cycle decomposition algorithm* which transforms an element-by-element definition of a permutation into a product of disjoint cycles written in compact cycle notation. Let's take a look at the algorithm.

Algorithm 1: Cycle Decomposition Algorithm

INPUT: Begin with a specific permutation $\pi : [n] \to [n]$

ALGORITHM STEPS:

1. Write an open left parenthesis to begin each new cycle. Then find the smallest element of $[n] = \{1, 2, 3, ..., n\}$ that is not yet used in a previous cycle - let's call this $i \in [n]$. Put this element immediately to the right of your open left parenthesis

   $$(\ i$$

   We start each cycle decomposition with $i = 1$ so that the first cycle we create always begins in the form $(\ 1$

2. Find the output value of π on input i. Call this $\pi(i) = j$. If the permutation maps i to itself with $j = i$, then close the cycle with the right closed parenthesis. This is a cycle of length 1. Return to step 1 in this algorithm. If the permutation sends output i to a different number so that $j = \pi(i) \neq i$, then capture the output j directly to the right of the value of i in the current cycle

   $$(\ i \ j$$

3. Find the output value of $\pi(j) = \pi(\pi(i))$. Call this $\pi(j) = k$. If the permutation maps k back to our first element i so that $k = i$, then end the cycle with the right closed parenthesis and return to step 1 of this algorithm. This is called a cycle of length 2. If the permutation sends j to a different number than i with $k = \pi(j) \neq i$, then write the output k directly to the right of the value of j in the current cycle

   $$(\ i \ j \ k$$

   and repeat this step until the cycle ends.

OUTPUT: The complete cycle notation of the permutation π.

EXAMPLE 10

Let's apply this general algorithm to our specific example of shuffling the 13 hearts cards from a standard 52-card deck. Recall that the Cauchy two line definition of our shuffle permutation is given as

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 10 & 11 & 12 & 4 & 2 & 9 & 3 & 13 & 6 & 7 & 5 & 1 & 8 \end{pmatrix}.$$

In step 1 of our algorithm, we find the smallest value of $i \in [13] = \{1, 2, 3, ..., 13\}$ that we haven't yet used. At the start of our work, we set $i = 1$ and write

$$(\ 1$$

Now we progress onto step 2 of our algorithm. We see $\tau(1) = 10 \neq 1$ so we write

$$(\ 1\ \ 10$$

We move down to step 3 of our algorithm and confirm that $\pi(10) = \pi(\pi(1)) = 7 \neq 1$ so we write

$$(\ 1\ \ 10\ \ 7$$

We continue in this manner until we end the first cycle with

$$(\ 1\ \ 10\ \ 7\ \ 3\ \ 12\ \ )$$

After we close the first cycle, let's cross out all the elements of our set [13] that show up in our first cycle:

$$\{\cancel{1}, 2, \cancel{3}, 4, 5, 6, \cancel{7}, 8, 9, \cancel{10}, 11, \cancel{12}, 13\}$$

Now, we can look for the smallest element that we have not yet used in our cycle decomposition. In this case we see that 2 remains unused so we follow our algorithm to write the second cycle directly to the right of our first cycle in the form

$$(\ 1\ \ 10\ \ 7\ \ 3\ \ 12\ \ )\ (\ 2\ \ 11\ \ 5\ \ )$$

We continue this process until all elements $[n]$ show up in exactly one cycle. Using this cycle decomposition algorithm, we produce the complete cycle notation for our shuffle example given by

$$(\ 1\ \ 10\ \ 7\ \ 3\ \ 12\ \ )\ (\ 2\ \ 11\ \ 5\ \ )\ (\ 4\ \ )\ (\ 6\ \ 9\ \ )\ (\ 8\ \ 13\ \ )$$

We adopt the convention that the way we order the distinct cycles of each permutation does not change the meaning of the definition so that

$$(1\ 10\ 7\ 3\ 12\,)\,(\,2\ 11\ 5\,)\,(\,4\,)\,(\,6\ 9\,)\,(\,8\ 13\,) = (\,8\ 13\,)\,(\,4\,)\,(\,2\ 11\ 5\,)\,(\,6\ 9\,)\,(1\ 10\ 7\ 3\ 12\,)$$

Each cycle also can be written in different a different order if we choose different starting points for our algorithm so that

$$(1\ 10\ 7\ 3\ 12\,)\,(\,2\ 11\ 5\,)\,(\,4\,)\,(\,6\ 9\,)\,(\,8\ 13\,) = (7\ 3\ 12\ 1\ 10\,)\,(\,5\ 2\ 11\,)\,(\,4\,)\,(\,9\ 6\,)\,(\,8\ 13\,)$$

In this notation, we say that *1-cycle* is a cycle that has length one and represents the case where a permutation sends a specific element back to itself. In complete cycle notation, we list every cycle to define the permutation completely. However, we may find it useful to leave out 1-cycles to write our permutation using *compact cycle notation*. For the case of our shuffle example, we have

$$\underbrace{(1\ 10\ 7\ 3\ 12\,)\,(\,2\ 11\ 5\,)\,(\,4\,)\,(\,6\ 9\,)\,(\,8\ 13\,)}_{\text{complete cycle notation}} = \underbrace{(1\ 10\ 7\ 3\ 12\,)\,(\,2\ 11\ 5\,)\,(\,6\ 9\,)\,(\,8\ 13\,)}_{\text{compact cycle notation}}$$

Using the cycle decomposition algorithm, we can write every permutation as a composition of disjoint cycles. This realization is worthy of a special title.

Theorem 2: Cycle Decomposition of Permutations

Let $n \in \mathbb{N}$. Every permutation in S_n can be written as a product of disjoint cycles and this representation is unique, except for the ordering of each cycle in the decomposition.

Let's use an analogy from the world of the English language. Let's think about the set of permutations in S_n as analogous to the set of sentences with n letters. This cycle decomposition theorem states that the individual cycles are analogous to the words we use to construct sentences. The $k-$cycles in S_n give us the power to construct any permutation as the product (i.e. composition) of $k-$cycles just like we construct sentences by stringing together words.

Another analogy might be helpful, this time from the world of arithmetic. Recall the prime factorization theorem states that we can decompose every composite number as a product of prime numbers. The individual factors are the prime numbers which, when combined together via multiplication, form the given composite number. In this case, our theorem indicates that every permutation can be decomposed into the product of factors called cycles.

Another way to think about our cycle decomposition algorithm is to view it through the lens of shuffling cards. Remember our question about the minimum number of shuffling movements that generate all possible orderings of a deck of cards? This algorithm indicates that using the set of all cycles, we can generate every possible permutation in S_n. Since not all permutations are cycles, we see that a strict subset of permutations generates all other permutations. This implies that the minimum number of permutations needed to generate the entire set S_n is strictly less than $n!$ so that we can generate all permutations by starting with a smaller subset. We don't yet know exactly how small that minimum set might be. To get more precise, let's take a closer look at a specific set of cycles that turn out to be quite powerful.

Definition 6: Transpositions

Let $n \in \mathbb{N}$. A *transposition*, also known as a *2-cycle*, is a permutation of length 2 that swaps two elements in $[n]$ and leaves the remaining $(n-2)$ elements fixed.

Let's list all transpositions (i.e. $2-$cycles) in S_2, S_3, S_4, and S_5 to get a better sense of these special permutations that swap two elements. In our exploration, we use the same numbering systems presented in Examples 4, 5, and 6 above. It's worth noting that for S_1, we have no transpositions since that set has a single element, the identity permutation, which sends 1 to itself. The first nontrivial case of a set of permutations that includes at least one transposition is that of S_2.

EXAMPLE 11

In the set S_2, we have exactly one transposition written as

$$\pi_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (\ 1\ \ 2\ ).$$

EXAMPLE 12

We have three unique transpositions in the set S_3 which are given by

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (\ 2\ \ 3\ )}_{\pi_4}, \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (\ 1\ \ 3\ )}_{\pi_5}, \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (\ 1\ \ 2\ )}_{\pi_6}.$$

EXAMPLE 13

There are six unique 2−cycles in S_4 including each of the following functions:

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (\ 3\ \ 4\ )}_{\pi_{13}}, \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (\ 2\ \ 4\ )}_{\pi_{14}},$$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (\ 2\ \ 3\ )}_{\pi_{15}}, \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = (\ 1\ \ 4\ )}_{\pi_{16}},$$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (\ 1\ \ 3\ )}_{\pi_{17}}, \quad \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (\ 1\ \ 2\ )}_{\pi_{18}}.$$

EXAMPLE 14

There are exactly ten permutations of length 2 in S_5, which we can write as:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (\ 4\ \ 5\ ), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} = (\ 3\ \ 5\ ),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} = (\ 3\ \ 4\ ), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = (\ 2\ \ 5\ ),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (\ 2\ \ 4\ ), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = (\ 2\ \ 3\ ),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix} = (\ 1\ \ 5\ ), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} = (\ 1\ \ 4\ ),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = (\ 1\ \ 3\ ), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} = (\ 1\ \ 2\ ).$$

Let's create a table of values to summarize our results from Examples 10, 11, 12, and 13 above.

n	S_n	Number of 2−cycles
1	S_1	0
2	S_2	1
3	S_3	3
4	S_4	6
5	S_5	10

We might recognize the sequence $1, 3, 6, 10$ as a famous pattern in arithmetic that represents the sum of the first few integers:

$$\begin{aligned} 1 &= 1, \\ 3 &= 1 + 2, \\ 6 &= 1 + 2 + 3, \\ 10 &= 1 + 2 + 3 + 4. \end{aligned}$$

What if we use these observations to make a guess for the number of 2−cycles in S_6, S_7, or S_8 by extending our pattern? Let's our guesses for the next few rows or our table below.

n	S_n	Number of 2−cycles
6	S_6	$15 = 1 + 2 + 3 + 4 + 5$
7	S_7	$21 = 1 + 2 + 3 + 4 + 5 + 6$
8	S_8	$28 = 1 + 2 + 3 + 4 + 5 + 6 + 7$

In each line of our table, we notice that the last summand in the calculation is one less than the value of n. This leads to a conjecture for the general count of the total number of transposition in S_n for any $n \in \mathbb{N}$ using the following formula:

$$\text{Number of transpositions in } S_n \;=\; \sum_{i=1}^{(n-1)} i = 1 + 2 + 3 + \cdots + (n-1) = \frac{(n-1)n}{2}$$

We might feel a sense of awe to realize that this count of the total number of transpositions in the set S_n is equal to the number of ways to choose 2 unique elements from the set $[n]$. This is exactly what the triangular number is designed to count. We can use Pascal's triangle to calculate this number, if we would like.

What other patterns can we discover?

We can ask ourselves a fun question about the set of transpositions: How many permutations can we generate from the set of 2−cycles? One fun way to explore this question is to think critically about the Cycle Decomposition of Permutation Theorem 2 which states that every permutation can be uniquely written as the product of disjoint cycles. But we have seen that not all cycles are transpositions. Thus, if we want to get a sense of which permutations we can generate using transpositions, we might want to see if we can generate cycles of length k where $k > 2$ by taking products of transpositions. To explore this question, let's consider some examples in S_3, S_4, and S_5.

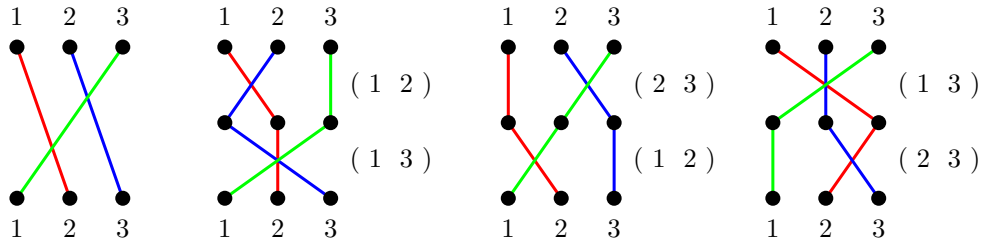
EXAMPLE 15

The set S_3 has exactly 6 elements including one identity permutation, three transpositions, and $2! = 2$ cycles of length 3. With little thought, we can decompose

each of these 3−cycles as a product of transpositions. Let's begin by analyzing the 3−cycles $\pi_2 \in S_3$ from Example 6 in this section. We recall that

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (\ 1\ \ 2\ \ 3\ ).$$

To write this 3−cycle as a product of 2−cycles, let's draw a permutation diagram and develop a color code for the connections between the input elements and the output elements. We use this coloring system as a heuristic to map the trajectory of each element and verify equivalence between the original map and our suggested transposition decompostions. Below, we present some diagrams that provide multiple options for how we might decompose our 3−cycle into a product of two cycles.



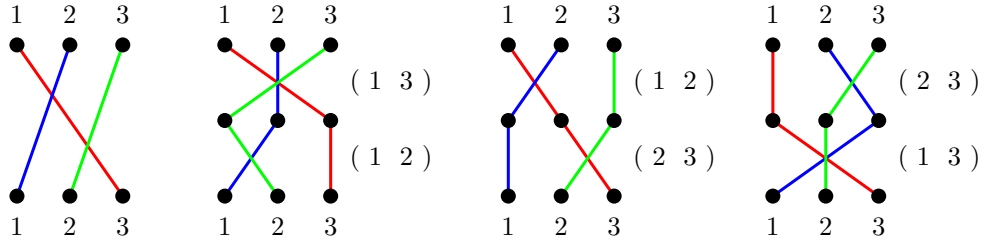
Using our notations, we write permutation π_2 as a product of transpositions:

$$\pi_2 = (\ 1\ \ 2\ \ 3\ ) = \underbrace{(\ 1\ \ 3\ ) \cdot (\ 1\ \ 2\ )}_{\text{Option 1}} = \underbrace{(\ 1\ \ 2\ ) \cdot (\ 2\ \ 3\ )}_{\text{Option 2}} = \underbrace{(\ 2\ \ 3\ ) \cdot (\ 1\ \ 3\ )}_{\text{Option 3}}$$

Let's write the other 3−cycle $\pi_3 \in S_3$ as a product of transpositions, where

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (\ 1\ \ 3\ \ 2\ ).$$

Again, we draw and color some permutations diagrams to get a better idea of how to create possible transposition decompositions of π_3:



Once again, we can write each of these options using cycle notation to see that

$$\pi_3 = (\ 1\ \ 3\ \ 2\ ) = \underbrace{(\ 1\ \ 2\ ) \cdot (\ 1\ \ 3\ )}_{\text{Option 1}} = \underbrace{(\ 2\ \ 3\ ) \cdot (\ 1\ \ 2\ )}_{\text{Option 2}} = \underbrace{(\ 2\ \ 3\ ) \cdot (\ 1\ \ 3\ )}_{\text{Option 3}}$$

If we study Example 14 above more closely, we might come to realize that the three listed options are the only ways we can decompose each 3−cycle into a product of transpositions where each unique transposition shows up only once in the composition. Rearranging the order of the transpositions changes the output as does adding other transpositions to the list. With a little thought we might see that there are an infinite number of ways to do these decompositions if we allow ourselves to write a specific transposition more than once in the product. For now, however, let's continue to develop our intuition about how we can find transposition decompositions for $n-$cycles in S_n by leveling up to $n = 4$.

EXAMPLE 16

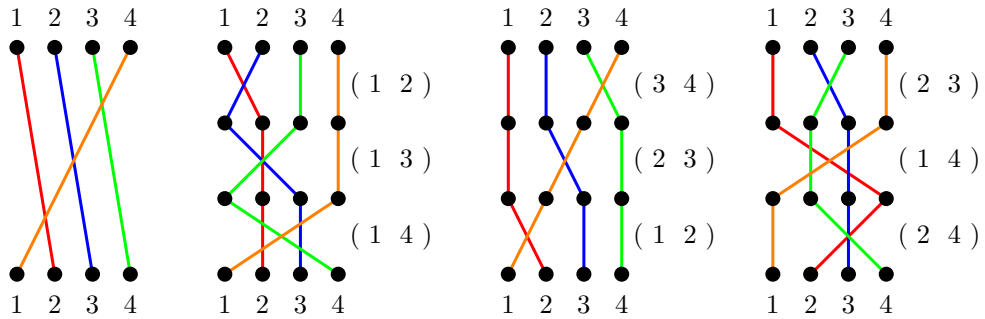
In our study of the 24 listed permutations in S_4 in Example 6 from this section, we see exactly $3! = 6$ cycles of length 4. Let's re-write these explicitly using the same labeling systems from Example 6:

$$\pi_{19} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (\ 1\ \ 2\ \ 3\ \ 4\ ), \quad \pi_{20} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (\ 1\ \ 3\ \ 2\ \ 4\ ),$$

$$\pi_{21} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (\ 1\ \ 2\ \ 4\ \ 3\ ), \quad \pi_{22} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (\ 1\ \ 4\ \ 2\ \ 3\ ),$$

$$\pi_{23} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (\ 1\ \ 3\ \ 4\ \ 2\ ), \quad \pi_{24} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (\ 1\ \ 4\ \ 3\ \ 2\ ).$$

To see how we can decompose a given 4−cycle into the product of transpositions, let's consider the permutation $\pi_{19} \in S_4$.



Option 1 Option 2 Option 3

Let's express these three decompositions of $\pi_{19} \in S_4$ into the product of transpositions via compact cycle and product notations:

$$\pi_{19} = \underbrace{(\ 1\ \ 4\ ) \cdot (\ 1\ \ 3\ ) \cdot (\ 1\ \ 2\ )}_{\text{Option 1}} = \underbrace{(\ 1\ \ 2\ ) \cdot (\ 2\ \ 3\ ) \cdot (\ 3\ \ 4\ )}_{\text{Option 2}} = \underbrace{(\ 2\ \ 4\ ) \cdot (\ 1\ \ 4\ ) \cdot (\ 2\ \ 3\ )}_{\text{Option 3}}$$

The decompositions listed in Example 15 are not the only options available to write π_{19} as a product of transpositions. One fun question for further exploration is to find out how many unique ways can we write a given 4−cycle as a product of transpositions such that no one transposition shows up more than once in that

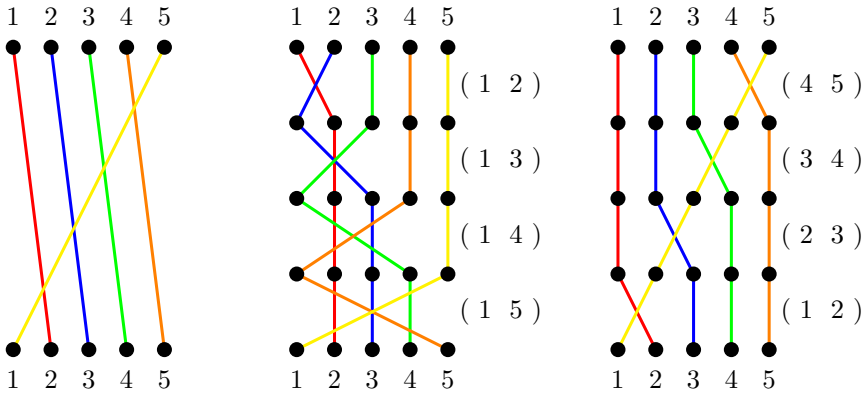
decomposition. To come up with a good conjecture, we might decompose each of the six 4−cycles in S_4 as product(s) of transpositions. Both of these exercises (and many others) are provided in the Beginning-Level exercises below. Let's end the author-driven exploration of transposition decompositions of $n-$cycles in S_n by leveling up one more time to the case when $n = 5$.

EXAMPLE 17

Based on Theorem 1 from this section, we know there are 5! permutations in S_5. Of those 120 elements, there are $4! = 24$ cycles of length 5. Let's look at a couple of options to decompose two of those 5−cycles into a product of transpositions to get some insights into the process. Let's start by studying the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (\ 1\ \ 2\ \ 3\ \ 4\ \ 5\ ),$$

Let's use our permutation-diagram heuristic along with the process of coloring the links between elements to come up with some possible transposition decompositions:



Option 1 Option 2

Using these diagrams, we can write

$$(\ 1\ \ 2\ \ 3\ \ 4\ \ 5\ ) = \underbrace{(\ 1\ \ 5\ ) \cdot (\ 1\ \ 4\ ) \cdot (\ 1\ \ 3\ ) \cdot (\ 1\ \ 2\ )}_{\text{Option 1}}$$

$$= \underbrace{(\ 1\ \ 2\ ) \cdot (\ 2\ \ 3\ ) \cdot (\ 3\ \ 4\ ) \cdot (\ 4\ \ 5\ )}_{\text{Option 2}}$$

As in the previous examples, we have more than two possible transposition decompositions for each 5−cycle in S_5. Please explore more about this in the corresponding adventures suggested in the Undergraduate-level exercises below.

Let's find some fun patterns in Examples 14, 15, and 16. Specifically, when we decompose every $n-$cycle in S_n as a product of transpositions, we have more than one way to do this. In other words, for any $k \in \mathbb{N}$ where $k > 2$, there are many possible ways to write a specific cycle of length k as a product of 2−cycles. This observation leads to a fascinating mathematical theorem.

Theorem 3: Transpositions Generate All Permutations

Let $n \in \mathbb{N}$. Every element of S_n can be decomposed as a product of transpositions.

Proof. Let $n \in \mathbb{N}$. Notice that for $n = 1$ we have only the identity permutation (there are no 2-cycles in S_1) and for $n = 2$ we have a single 2−cycle in S_2. Thus, we can safely suppose $n > 2$. To prove this theorem, let's restate some of the discoveries we've made in our work. First, we know from our Cycle Decomposition Algorithm that any permutation in S_n can be written as a product of disjoint cycles and this decomposition is unique (up to re-ordering the cycles). Moreover, for any $2 < k \leq n$, we can decompose any k−cycle into a product of transpositions. One way to do this is to state a general algorithm that follows the patterns from option 1 and 2 in Example 14 -16 above.

Let's start with the case that $k = 3$. For some $m_1, m_2, m_3 \in [n]$, any 3−cycle that pops out from the Cycle Decomposition algorithm will take the form $(\ m_1 \ \ m_2 \ \ m_3 \ )$. Notice that we will always be able to decompose such a 3−cycle using at least two different options

$$(\ m_1 \ \ m_2 \ \ m_3 \ ) = \underbrace{(\ m_1 \ \ m_3 \ ) \cdot (\ m_1 \ \ m_2 \ )}_{\text{Option 1}} = \underbrace{(\ m_1 \ \ m_2 \ ) \cdot (\ m_2 \ \ m_3 \ )}_{\text{Option 2}}$$

This same pattern holds for all 4−cycles in the form $(\ m_1 \ \ m_2 \ \ m_3 \ \ m_4 \ )$ for any $m_1, m_2, m_3, m_4 \in [n]$. Specifically, we see that

$$(\ m_1 \ \ m_2 \ \ m_3 \ \ m_4 \ ) = \underbrace{(\ m_1 \ \ m_4 \ ) \cdot (\ m_1 \ \ m_3 \ ) \cdot (\ m_1 \ \ m_2 \ )}_{\text{Option 1}}$$

$$= \underbrace{(\ m_1 \ \ m_2 \ ) \cdot (\ m_2 \ \ m_3 \ ) \cdot (\ m_3 \ \ m_4 \ )}_{\text{Option 2}}$$

We can extend this pattern to decompose any 5−cycle with

$$(\ m_1 \ \ m_2 \ \ m_3 \ \ m_4 \ \ m_5 \ ) = \underbrace{(\ m_1 \ \ m_5 \ ) \cdot (\ m_1 \ \ m_4 \ ) \cdot (\ m_1 \ \ m_3 \ ) \cdot (\ m_1 \ \ m_2 \ )}_{\text{Option 1}}$$

$$= \underbrace{(\ m_1 \ \ m_2 \ ) \cdot (\ m_2 \ \ m_3 \ ) \cdot (\ m_3 \ \ m_4 \ ) \cdot (\ m_4 \ \ m_5 \ )}_{\text{Option 2}}$$

where $m_1, m_2, m_3, m_4, m_5 \in [n]$. We generalize this process to decompose any k−cycle into the product of transpositions using either of these two options with

$$(\ m_1 \ \ m_2 \ \ \cdots \ \ m_{k-1} \ \ m_k \ ) = \underbrace{(\ m_1 \ \ m_k \ ) \cdot (\ m_1 \ \ m_{k-1} \ ) \cdots (\ m_1 \ \ m_3 \ ) \cdot (\ m_1 \ \ m_2 \ )}_{\text{Option 1}}$$

$$= \underbrace{(m_1 \ \ m_2 \ ) \cdot (m_2 \ \ m_3 \ ) \cdots (m_{k-2} \ \ m_{k-1} \ ) \cdot (m_{k-1} \ \ m_k \ )}_{\text{Option 2}}$$

Since this process works for any k−cycle and we know that every permutation can be uniquely expressed as a product of cycles, we see that we can decompose every permutation as a product of transpositions. This is what we wanted to show. □

Theorem 3 above highlights a fascinating feature of transpositions in S_n which is that $2-$cycles generate all of S_n. If we add the restriction that each unique $2-$cycle in the product can only appear once, then no matter how many different options we have for the transposition decomposition, the number of transpositions will be constant across all options. For instance, we saw in Example 14 that for $3-$cycles in S_3, we had three possible transposition decompositions $\pi_2, \pi_3 \in S_3$. In each case, there were exactly two transpositions in the product. For $4-$cycles in S_4, we saw in Example 15 that each of the three listed options for possible transposition decompositions had three $2-$cycles in the product.

In the Beginner-Level exercises below, we explore many other options for decomposing $4-$cycles as the product of transpositions so that every transposition shows up no more than once. However, no matter how we do this, there will always be three $2-$cycles. In Example 16, we had that $5-$cycles can be written as the product of four unique $2-$cycles. This pattern holds true for any transposition decomposition. In other words, although we have many ways to decompose a given permutation into the product of transposition, there is an underlying characteristic that holds constant across any transposition decomposition that we choose. We can formalize this observation using the following definition.

Definition 7: Sign of a Permutation Using Transpositions

Let $n \in \mathbb{N}$ and suppose $\pi \in S_n$. We define the sign of a permutation as

$$\text{sgn}\,(\pi) = (-1)^m$$

where m counts the number of factors in the decomposition of π into a product of transpositions.

Let's extend our work from examples 14, 15, and 16 to figure out if there is a unique way to decompose a specific permutation into a product of transpositions.

EXAMPLE 18

We can use our work from example 14 to produce a complete transposition decomposition of permutation in S_3. Once we do so, we can calculate the sign of each permutation using transpositions by counting of the number of $2-$cycles in the decomposition(s) of each element of S_3 to find that

$$\begin{aligned}
\pi_1 &= (\,1\,)\,(\,2\,)\,(\,3\,) && \Longrightarrow && \text{sgn}(\pi_1) = (-1)^0 = +1 \\
\pi_2 &= (\,1\ \ 2\ \ 3\,) = (\,1\ \ 3\,)\cdot(\,1\ \ 2\,) && \Longrightarrow && \text{sgn}(\pi_2) = (-1)^2 = +1 \\
\pi_3 &= (\,1\ \ 3\ \ 2\,) = (\,1\ \ 2\,)\cdot(\,1\ \ 3\,) && \Longrightarrow && \text{sgn}(\pi_3) = (-1)^2 = +1 \\
\pi_4 &= (\,2\ \ 3\,) && \Longrightarrow && \text{sgn}(\pi_4) = (-1)^1 = -1 \\
\pi_5 &= (\,1\ \ 3\,) && \Longrightarrow && \text{sgn}(\pi_5) = (-1)^1 = -1 \\
\pi_6 &= (\,1\ \ 2\,) && \Longrightarrow && \text{sgn}(\pi_6) = (-1)^1 = -1
\end{aligned}$$

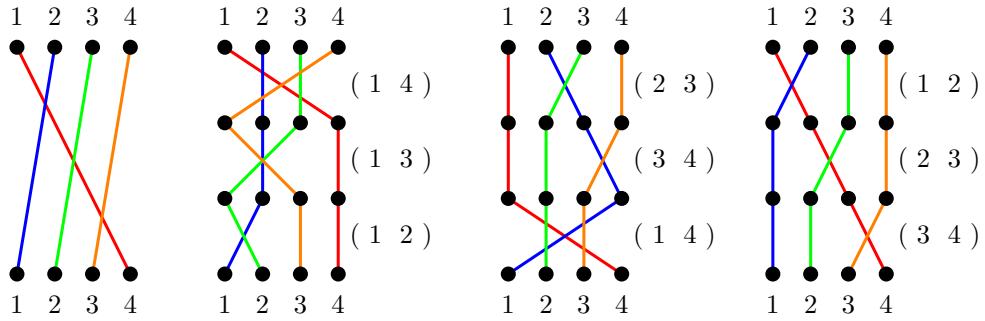
.

EXAMPLE 19

Let's find the sign of permutation $\pi_{24} \in S_4$ from Example 6 of this Lesson, where

$$\pi_{24} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (\ 1\ \ 4\ \ 3\ \ 2\ ).$$

We can use permutation diagrams to generate multiple options to decompose π_{24} into the product of transpositions, as seen below



Option 1 Option 2 Option 3

We write these three decompositions of $\pi_{24} \in S_4$ as a product below:

$$\pi_{24} = \underbrace{(\ 1\ \ 2\ ) \cdot (\ 1\ \ 3\ ) \cdot (\ 1\ \ 4\ )}_{\text{Option 1}} = \underbrace{(\ 1\ \ 4\ ) \cdot (\ 3\ \ 4\ ) \cdot (\ 2\ \ 3\ )}_{\text{Option 2}} = \underbrace{(\ 3\ \ 4\ ) \cdot (\ 2\ \ 3\ ) \cdot (\ 1\ \ 2\ )}_{\text{Option 3}}$$

Each of our three options for transposition decompositions of π_{24} has $m = 3$ factors. We calculate the sign of π_{24} using our formula from Definition 7 as

$$\text{sgn}\,(\pi_{24}) = (-1)^m = (-1)^3 = -1.$$

We compare the sign of π_{24} to the sign of the permutation $\pi_{12} \in S_4$ given by

$$\pi_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (\ 1\ \ 4\ ) \cdot (\ 2\ \ 3\ ).$$

This transposition decomposition for $\pi_{12} \in S_4$ has exactly $m = 2$ transpositions and we calculate that

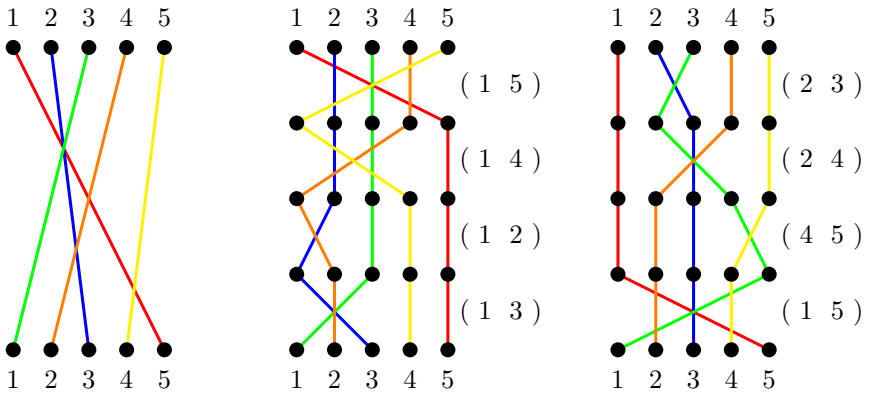
$$\text{sgn}\,(\pi_{12}) = (-1)^m = (-1)^2 = +1.$$

EXAMPLE 20

To end this exploration, let's look at a different 5−cycle in S_5 defined as:

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} = (\ 1\ \ 5\ \ 4\ \ 2\ \ 3\ ),$$

To figure out how we might decompose this 5−cycle into compositions of 2−cycles, let's use our permutation-diagram heuristic along with the process of coloring the links between elements.



Option 1 Option 2

Let's translate our diagrams into cycle notation as follows

$$(1\ 5\ 4\ 2\ 3) = \underbrace{(1\ 5)\cdot(1\ 4)\cdot(1\ 2)\cdot(1\ 3)}_{\text{Option 1}} = \underbrace{(2\ 3)\cdot(2\ 4)\cdot(4\ 5)\cdot(1\ 5)}_{\text{Option 2}}$$

In each of these two options, we decompose β in a product of $m = 4$ transpositions. Based on the formula for the sign of β given in Definition 7, we see that

$$\text{sgn}(\beta) = (-1)^m = (-1)^4 = +1.$$

EXAMPLE 21

Let's revisit our card shuffle example that we explored in Example 2 and 9 of this lesson. In that example, we studied the permutation $\tau \in S_{13}$ defined as follows:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 10 & 11 & 12 & 4 & 2 & 9 & 3 & 13 & 6 & 7 & 5 & 1 & 8 \end{pmatrix}$$

$$= (1\ 10\ 7\ 3\ 12)\ (2\ 11\ 5)\ (6\ 9)\ (8\ 13)$$

We can further decompose this permutation into a product of transpositions by using either option 1 or 2 highlighted at our proof of Theorem 3 from this lesson. Doing so, we see that

$$\tau = \underbrace{(1\ 10)\cdot(1\ 7)\cdot(1\ 3)\cdot(1\ 12)\cdot(2\ 5)\cdot(2\ 11)\cdot(6\ 9)\cdot(8\ 13)}_{\text{Option 1}}$$

$$= \underbrace{(1\ 10)\cdot(7\ 10)\cdot(3\ 7)\cdot(3\ 12)\cdot(2\ 11)\cdot(5\ 11)\cdot(6\ 9)\cdot(8\ 13)}_{\text{Option 2}}$$

In either case, we have $m = 8$ transpositions in the product and we calculate

$$\text{sgn}(\tau) = (-1)^m = (-1)^8 = +1$$

We see from our work in examples 14, 15, and 16 that there is not a unique way to decompose a specific permutation $\pi \in S_n$ into a product of transpositions. However, even though this decomposition process is not unique, the parity (evenness or oddness) of all decompositions of π is the same. In other words, either every possible transposition decomposition of π will feature an even number transpositions or every possible transposition decomposition of π will have an odd number of transpositions. This property ensures that our chosen definition of the sign of a permutation assigns a unique value to each individual permutation (i.e. the sign of a permutation is well-defined).

Definition 8: Parity of a Permutation

Let $n \in \mathbb{N}$. A permutation $\pi \in S_n$ is *even* if it can be written as the product of an even number of transpositions. Alternatively, a permutation $\sigma \in S_n$ is *odd* if σ can be written as the product of an odd number of transpositions. The parity of a permutation refers to the evenness or oddness of that permutation.

In the definition above, we borrow terminology from the study of integers. The parity of an integer refers to whether an integer is even or odd. In this lesson, Definition 7 of the sign of a permutation can be a bit subtle due to the nonuniqueness of the decomposition of a given permutation into products of transpositions. As we saw in examples 14 - 20, there are many ways to decompose a single permutation into a product of $2-$cycles. However, no matter which decomposition we produce, the number of individual transpositions that combine to form a single permutation will always be either even or odd.

One of the fascinating features of the transposition decomposition process is that no matter how we write a given permutation as a product of $2-$cycles, the number of transpositions will always be either even or odd for that specific permutation. We know that (-1) raised to any odd number will always output a negative sign of while (-1) raised to any even power always outputs a positive sign. This property ensures that we can safely define the sign of a permutation without worrying about which specific sequence of factors we string together to form the transposition decomposition of a given permutation. In other words, although there maybe some variation in the specific decomposition we choose, the sign we calculate will always be the same and represents a type of immutable characteristic of each permutation, kind of like a thumbprint or eye color on a human being.

What other methods can we use to develop the sign of a permutation?

The idea of the sign of a permutation is interesting enough that we might want to develop this idea using multiple approaches. Rather than developing the concept of the sign of a permutation using the transposition decomposition approach, we can alternatively create a measurement of how much a permutation in S_n forces the first n integers in the set $[n] = \{1, 2, 3, ..., n\} \subset \mathbb{N}$ out of their natural order. We explore these concept using the idea of inversions.

In the English language, we say something is inverted when that object is flipped around from its original position. Using this intuition, we might say that a permutation $\pi \in S_n$ inverts a pair of integers $i, k \in [n]$ with $1 \leq i < k \leq n$ if the order relation between the outputs $\pi(i)$ and $\pi(k)$ are the opposite from the order relations between inputs i and k. Let's formalize this intuition as a definition.

Definition 9: Inversion of a pair (i, j) with respect to π

Let $\pi \in S_n$. Suppose that $i, j \in [n]$ are chosen such that $1 \leq i < j \leq n$. We call the pair (i, j) an *inversion* with respect to π if and only if

$$i < j \qquad \text{but} \qquad \pi(i) > \pi(j).$$

We call the pair (i, j) an inversion with respect to a given permutation π if the images $\pi(i)$ and $\pi(j)$ are in the opposite order from their natural order in $\mathbb{N}$. By developing the concept of inversions, we can count of how out-of-order the output elements of a permutation are compared to the input elements. This count is the number of inversion pairs in the permutation.

When counting the number of possible inversions in a given permutation, we start by exploring more about the natural order of elements in $[n] = \{1, 2, 3, ..., n\}$. The set $[n]$ has a total order between the elements that results in a chain of strict inequalities in the form:

$$1 < 2 < 3 < \cdots < (n-1) < n$$

This set of order relations represents more than n relations. For example, for the case that $n = 3$, we see the following relationship:

$$1 < 2 < 3 \qquad \Longrightarrow \qquad 1 < 2, \qquad 2 < 3, \qquad 1 < 3$$

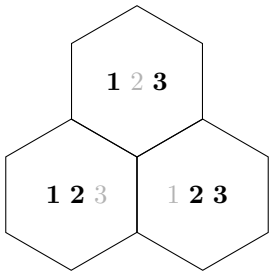
In other words, to study the number of inversions of a given permutation $\pi \in S_3$, we have three possible inversion pairs that we need to consider, each one of which corresponds to a strict inequality relation between the elements, written as

$$\underbrace{1 < 2}_{\text{1st order relation}} \iff \underbrace{(1, 2)}_{\text{1st Inversion Pair}}$$

$$\underbrace{2 < 3}_{\text{2nd order relation}} \iff \underbrace{(2, 3)}_{\text{2nd Inversion Pair}}$$

$$\underbrace{1 < 3}_{\text{3rd order relation}} \iff \underbrace{(1, 3)}_{\text{3rd Inversion Pair}}$$

We can visualize these order relations between the three different input pairs of the set S_3, we can use the following *place-based inversion diagram*:



We call the pair (i, k) an inversion with respect to the permutation $\pi \in S_3$ when the images $\pi(i)$ and $\pi(k)$ have inverted orders compared to the ordering of the preimages $i < k$.

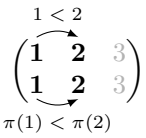
EXAMPLE 22

Let's recall the identity permutation in S_3, defined in Example 5 of this lesson as

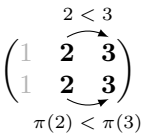
$$\pi_1 = (\,1\,)\,(\,2\,)\,(\,3\,).$$

The identity permutation $\pi_1 \in S_3$ preserves the natural ordering perfectly since it makes no changes. The order relation between each pair of input elements is identical to the order between the corresponding output elements.

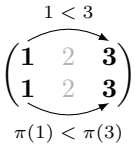
Inversion pair 1: No



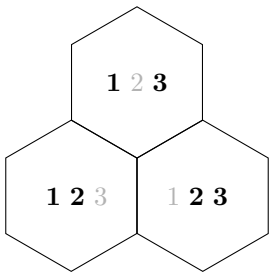
Inversion pair 2: No



Inversion pair 3: No



The place-based inversion diagram for $\pi_1 \in S_3$ is given as follows:



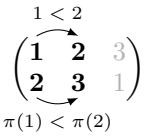
EXAMPLE 23

Next let's a look at the 3−cycle $\pi_2 \in S_3$ from Example 5 of this lesson given by

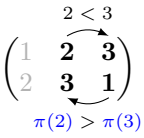
$$\pi_2 = (\ 1\ \ 2\ \ 3\ ).$$

The permutation $\pi_2 \in S_3$ changes the natural order between the input elements in the set $[3] = \{1, 2, 3\}$. Indeed, the order relations between each pair of input elements is different from the order between their corresponding output elements for this action.

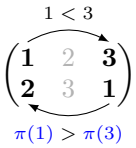
Inversion pair 1: No



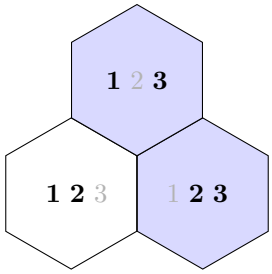
Inversion pair 2: Yes



Inversion pair 3: Yes



The place-based inversion diagram for $\pi_2 \in S_3$ is given as follows:



EXAMPLE 24

We continue by analyzing $\pi_3 \in S_3$ from Example 5 of this lesson given by

$$\pi_3 = (\ 1 \quad 3 \quad 2\ ).$$

Let's identify the inversions of $\pi_3 \in S_3$ by comparing the order relations between each pair of input elements with the order of the corresponding output elements.

Inversion pair 1: Yes

$$1 < 2 \qquad \begin{pmatrix} \mathbf{1} & \mathbf{2} & 3 \\ \mathbf{3} & \mathbf{1} & 2 \end{pmatrix} \qquad \pi(1) > \pi(2)$$

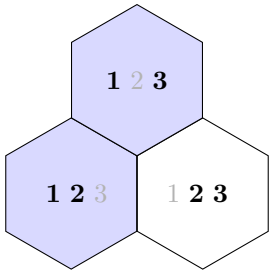
Inversion pair 2: No

$$2 < 3 \qquad \begin{pmatrix} 1 & \mathbf{2} & \mathbf{3} \\ 3 & \mathbf{1} & \mathbf{2} \end{pmatrix} \qquad \pi(2) < \pi(3)$$

Inversion pair 3: Yes

$$1 < 3 \qquad \begin{pmatrix} \mathbf{1} & 2 & \mathbf{3} \\ \mathbf{3} & 1 & \mathbf{2} \end{pmatrix} \qquad \pi(1) > \pi(3)$$

Below is the place-based inversion diagram for $\pi_3 \in S_3$:



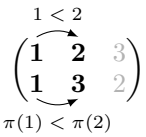
EXAMPLE 25

Next let's a look at the 2−cycle $\pi_4 \in S_3$ from Example 5 of this lesson given by

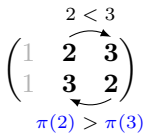
$$\pi_4 = (\ 2\ \ 3\ )$$

and let's identify the inversion pairs that show up in this permutation.

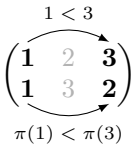
Inversion pair 1: No



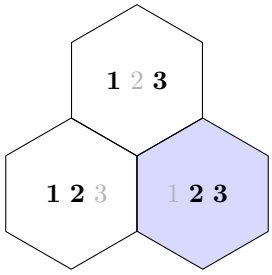
Inversion pair 2: Yes



Inversion pair 3: No



The place-based inversion diagram for $\pi_4 \in S_3$ is given as:



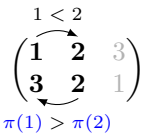
EXAMPLE 26

Let's look at the 2−cycle

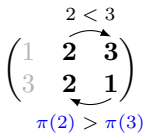
$$\pi_5 = (\ 1\ \ 3\ ).$$

All three inversion pairs show up in this permutation meaning the outputs are maximally out of order.

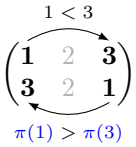
Inversion pair 1: Yes



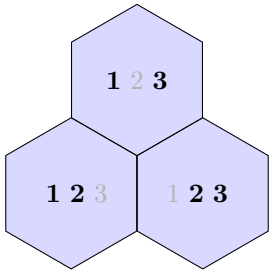
Inversion pair 2: Yes



Inversion pair 3: Yes



The place-based inversion diagram for $\pi_5 \in S_3$ is given as:



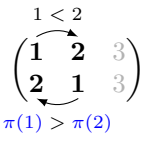
EXAMPLE 27

We complete our study of the inversion pairs that show up in S_3 by studying the final of 2−cycle

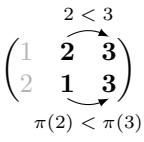
$$\pi_6 = \begin{pmatrix} 1 & 2 \end{pmatrix}$$

and let's identify the inversion pairs that show up in this permutation.

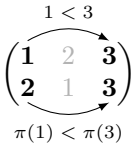
Inversion pair 1: Yes



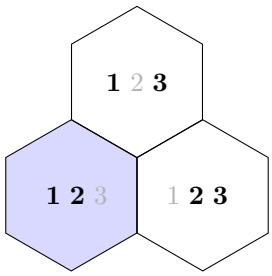
Inversion pair 2: No



Inversion pair 3: No



Our place-based inversion diagram for $\pi_6 \in S_3$ is given as:



Definition 10: Inversion set and inversion number of $\pi \in S_n$

Let $\pi \in S_n$ be given. We define the *inversion set* of π as

$$\text{Inv}(\pi) = \{(i,j) \, : \, i,j \in [n], i < j, \text{ and } \pi(i) > \pi(j)\}$$

Moreover, the *inversion number of* π, denoted as $\text{inv}(\pi)$, is the cardinality of the inversion set of π with

$$\text{inv}(\pi) = |\text{Inv}(\pi)|$$

In other words, the function $\text{inv} : S_n \to \mathbb{U}$ counts the number of elements in the inversion set of π.

EXAMPLE 28

Let's consider the set S_3, which has a total of $3! = 6$ permutations. From Examples 20 - 26 above, we know that:

$$\begin{aligned}
\text{Inv}(\pi_1) &= \emptyset &&\implies && \text{inv}(\pi_1) = 0 \\
\text{Inv}(\pi_2) &= \{(1,3),(2,3)\} &&\implies && \text{inv}(\pi_2) = 2 \\
\text{Inv}(\pi_3) &= \{(1,2),(1,3)\} &&\implies && \text{inv}(\pi_3) = 2 \\
\text{Inv}(\pi_4) &= \{(2,3)\} &&\implies && \text{inv}(\pi_4) = 1 \\
\text{Inv}(\pi_5) &= \{(1,2),(1,3),(2,3)\} &&\implies && \text{inv}(\pi_5) = 3 \\
\text{Inv}(\pi_6) &= \{(1,2)\} &&\implies && \text{inv}(\pi_6) = 1
\end{aligned}$$

The major goal of inversions, inversion sets, and inversion numbers is to develop a measurement of "how out of order are the outputs of this permutation?" From examples 21 - 36, we notice that the inversion number for permutations any $\pi \in S_3$ is bounded between $0 \leq \text{inv}(\pi) \leq 3$. The identity permutation has 0 inversions and has a zero out-of-order measurement. The permutation $\pi_5 \in S_3$ is maximally out of order with an inversion number of 3. We might try to generalize these observations to higher values of n. For example, we can ask: what are the ranges for inversion numbers for permutations $\pi \in S_n$ where $n \in \mathbb{N}$. To get insights into the answer to this question, let's take a look at one more case where $n = 4$.

EXAMPLE 29

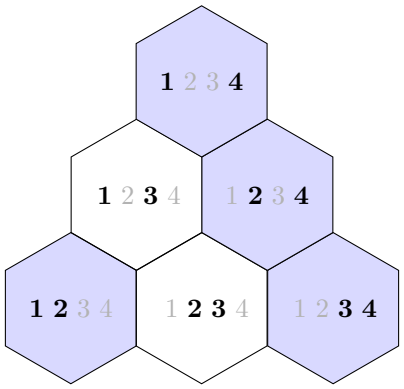
Let's use find the inversion number for a permutation in S_4 given by

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (\ 1 \ \ 3 \ \ 4\ ).$$

To figure out the inversion number for this permutation, we start by figuring out how many possible inversion pairs exist for elements of S_4. We use the chain of strict inequalities that fully define the total ordering on the set $[4]$ to find all possible inversion pairs:

$$\begin{aligned}
1 < 2 < 3 < 4 \quad &\implies \quad 1 < 2, \quad 2 < 3, \quad 3 < 4, \quad 1 < 3 \quad 2 < 4, \quad 1 < 4, \\
&\implies \quad (1,2) \quad (2,3) \quad (3,4) \quad (1,3) \quad (2,4) \quad (1,4).
\end{aligned}$$

We see that the six order relations for the set [4] correspond to six unique inversion pairs. We then test the individual output relations for π_4 for each of these six inversion pairs to produce a *place-based inversion diagram* for π_4 given below:



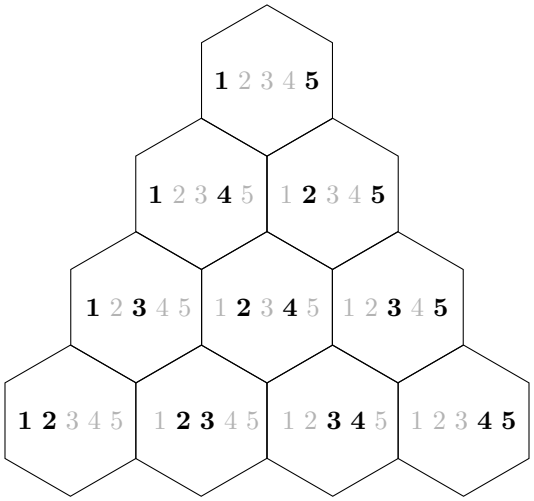
This diagram tells us which inversion pairs show up in π_4 and we conclude that

$$\text{Inv}(\pi_4) = \{(1,2),(3,4),(2,4),(1,4)\} \qquad \Longrightarrow \qquad \text{inv}(\pi_4) = 4.$$

Using our study of the $n = 3$ and $n = 4$ cases above, we might conjecture that for any $n \in \mathbb{N}$ and $\pi \in S_n$, we have lower and upper bounds for that permutation's inversion number given by

$$0 \leq \text{inv}(\pi) \leq \binom{n}{2} = \frac{(n-1)n}{2}$$

Moreover, we can extend the pattern for our placed-based inversion diagram when $n > 4$. In the $n = 5$ case, our place-based inversion diagram includes 10 possible inversion pairs and is given below:



These diagrams provide convenient and rapid access to all relevant inversion information and can be used to calculate inversion numbers quickly by counting the number of inversion pairs that are highlighted in the diagram. We can now use the inversion number measurement to provide an alternative way of calculating the sign of a permutation.

Definition 11: Sign of a Permutation using Inversions

The sign of a permutation π using inversions is given as

$$\text{sgn}(\pi) = (-1)^{\text{inv}(\pi)}.$$

We can write this another way:

$$\text{sgn}(\pi) = \begin{cases} +1 & \text{if there are an even number of inversions in the inversion set of } \pi, \\ -1 & \text{if there are an odd number of inversions in the inversion set of } \pi. \end{cases}$$

EXAMPLE 30

Let's find the sign of each permutation in S_3. We do so by recalling that

$$\begin{aligned}
\text{Inv}(\pi_1) &= \emptyset &&\Longrightarrow && \text{inv}(\pi_1) = 0 \\
\text{Inv}(\pi_2) &= \{(1,3),(2,3)\} &&\Longrightarrow && \text{inv}(\pi_2) = 2 \\
\text{Inv}(\pi_3) &= \{(1,2),(1,3)\} &&\Longrightarrow && \text{inv}(\pi_3) = 2 \\
\text{Inv}(\pi_4) &= \{(1,2),(1,3),(2,3)\} &&\Longrightarrow && \text{inv}(\pi_4) = 3 \\
\text{Inv}(\pi_5) &= \{(2,3)\} &&\Longrightarrow && \text{inv}(\pi_5) = 1 \\
\text{Inv}(\pi_6) &= \{(1,2)\} &&\Longrightarrow && \text{inv}(\pi_6) = 1
\end{aligned}$$

We can use this data to confirm that

$$\begin{aligned}
\text{sgn}(\pi_1) &= (-1)^{\text{inv}(\pi_1)} = (-1)^0 = +1 \\
\text{sgn}(\pi_2) &= (-1)^{\text{inv}(\pi_2)} = (-1)^2 = +1 \\
\text{sgn}(\pi_3) &= (-1)^{\text{inv}(\pi_3)} = (-1)^2 = +1 \\
\text{sgn}(\pi_4) &= (-1)^{\text{inv}(\pi_4)} = (-1)^3 = -1 \\
\text{sgn}(\pi_5) &= (-1)^{\text{inv}(\pi_5)} = (-1)^1 = -1 \\
\text{sgn}(\pi_6) &= (-1)^{\text{inv}(\pi_6)} = (-1)^1 = -1
\end{aligned}$$

This will come in very helpful in our development of the determinant function in Chapter 7. Write compelling conclusion to wrap up lesson and prime the pump for the future lessons (start making connections for the future).

Introduction to Permutations Problem Set

In the problem set, include introduction to the 12-fold way. This might include undergraduate level problems (which I provide solutions to) and graduate level problems which I do not provide solutions to. That way we have low floor, high ceiling exercises that satisfy both young students and more advanced thinkers simultaneously.

Beginner-Level Problems: These are problems that might require anywhere from 5 minutes - 60 minutes for a novice to make progress on. The goal of these problems is to help deepen your intuition about core topics covered in the material.

1. Let σ, τ be in S_6. Find the cycle decompositions of a few different compositions $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \tau^2\sigma$
2. Let σ, τ be in S_{16}. Find the cycle decompositions of a few different compositions $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \tau^2\sigma$
3. Compute the order of each permutation you found in the preceding exercises.
4. Write out the cycle decomposition for all elements in S_4.
5. Write out the cycle decomposition for all elements in S_5.
6. Show that the transposition $(1, 3)$ in S_3 can be written as a composition of the transpositions (12) and $(2, 3)$.
7. Show that any of the
$$\binom{4}{2} = \frac{4 \cdot 3}{2!} = 6$$
transposition in S_4 can be written as a composition of permutations from the following set of transpositions
$$\{(12), (2, 3), (3, 4)\}.$$
8. Decompose every element of S_4 as a composition of transpositions.
9. Decompose every element of S_5 as a composition of transpositions.
10. List all transpositions in S_6 and S_7.
11. Do we need all the transpositions? What redundancies exist between transpositions.
12. Let's define a minimal set of generators for S_n. Show that we can write any transposition in these sets in terms of a product of elements from our minimal set of generators.
13. Decompose all permutations in S_3 in terms of the transpositions in the minimal set of generators.
14. Decompose all permutations in S_4 in terms of the transpositions in the minimal set of generators.

15. Prove that $\sigma \in S_n$ has order 2 if and only if its cycle decomposition is a product of commuting 2−cycles.

16. Prove that the complete cycle notation produced by the Cycle Decomposition Algorithm is unique (up to recording of the cycles).

17. Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycle in the Cycle Decomposition of that element.

18. Prove that S_n combined with the product of permutations forms a group (as defined in abstract algebra).

19. Find the sign of every element of S_2, S_3, and S_4 using the transposition decomposition definition of the sign of a permutation.

20. Find the sign of every element in S_5 using the transposition decomposition definition.

21. Prove that although the transposition decomposition of an element in S_n is not unique, the parity of the number of transpositions in each decomposition is always the same so that the sign of a permutation is well-defined.

22. What if we remove the condition that each 2−cycle factor in the transposition decomposition must be unique? How does this effect the calculation of the sign? If options 1 and 2 yield an even number of factors, is it possible to get an odd number by introducing multiple copies of some of the 2−cycles?

23. Find the inversion sets for all elements of S_4 and use this to calculate the sign of each permutation in S_4. Compare your work with the transposition decomposition definition for the sign of each element.

24. Find the inversion sets for all elements of S_5 and use this to calculate the sign of each permutation in S_5. Compare your work with the transposition decomposition definition for the sign of each element.

25. One quick way to check if (i, j) is an inversion with respect to π is to calculate the ratio

$$\frac{\pi(i) - \pi(j)}{i - j}$$

If this ratio is less than 0, it means that (i, j) is an inversion with respect to π. On the other hand, if this ratio is greater than 0, then the pair (i, j) is not an inversion with respect to π. Show that this is a measurement of when a permutation inverts the input pair (i, k) if $i < k$ but $\pi(i) > \pi(k)$.

26. Show that the inversion number of a permutation is equal to the number of crossings in the permutation diagram.

27. Use Vandermonde Polynomial to prove the equivalence between our two definitions of the sign of a permutation.

28. Introduce dihedral groups and ask readers to identify which elements of S_n are included and which are excluded.

29. Prove that the set of even permutations form a subgroup of S_n.

How can I provide full solutions to my problem sets? Perhaps students can be involved with that project?

Intermediate-Level Problems (problems that likely require many hours or even few days for a novice to make progress on)

1. Count the number of $k-$cycles for $k = 1, 2, 3, ...n$. Then count the number of permutations in S_n that are not pure $k-$cycles.
2. How many different ways can you find to decompose a given $k-$cycle in S_n into the product of transpositions in S_n so that no transposition shows up more than once in that product? To get started, you might study $n-$cycles in S_n for $n = 3, 4, 5$ and generate a conjecture for your work. Then, come up with a general proof that justifies your approach.
3. Study the various sorting algorithms used in so much of popular computer science. Code up each of these algorithms for yourself. Then, discuss how each sorting algorithm related to Theorem 2 above.
4. How many different ways can you prove equivalence between our two definitions of the sign of a permutation? In other words, how many different proofs can you generate to show that
$$\text{sgn}(\pi) = (-1)^m = (-1)^{\text{inv}(\pi)}.$$
5. Conduct a study of the dihedral groups. Classify all dihedral groups for the first few values of N.
6. Learn how to solve a Rubik's Cube. Then, map your solutions back to the set S_n. How are permutations related to your solution algorithm. What is the minimum number of moves you need to be able to solve any rubik's cube? Why?

How are permutations related to matrices?

A. Discuss permutation matrices

B. Discuss the dihedral group

C. Show how permutation matrices can be used to create 2D and 3D graphics that include rotations, reflections, and symmetries of 2D/3D objects.

Advanced-Level Problems (problems that likely require many days, weeks, or even months of work for a novice make progress on and likely require support from resources that are not included in this manuscript)

1. Each of these rules adds a unique to other scenarios are quite interesting and yield some very fun mathematics. We can try to count how many possible ways exist in these cases. The mathematical study of counting objects is know as combinatorics. Concrete Mathematics by Donald Knuth or Enumerative Combinatorics, Volumes 1 and 2 by Richard Stanley. In that second book, there is a very fun set of mathematical problems known as the 12-fold way all about how to count the number of maps from a set of n objects into a set of m bins under various conditions. Write some good graduate-level practice problems that invites students to count the number of each type of map when we delete some of these rules.
2. Code up each and every sorting algorithm from the following list. How does each algorithm relate to the transposition decomposition of the permutation.