CHMC Advanced Group:
Symmetric Groups and the Fifteen Puzzle

Sep. 21, 2024

1 Introduction

Today, we'll consider a popular puzzle known as the Fifteen Puzzle. In this puzzle, you have a 4 by 4 grid with tiles labelled $1, 2, \ldots, 15$ and one empty space used to slide the tiles around. Your goal is to slide the tiles to get from some random configuration like this:

7	11	9	10
14	13	2	3
1	6	15	8
12	4	5	

to the "solved" configuration like this (we may also refer to this as the "neutral" configuration or "identity" configuration):

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Now for many an eager puzzle solver, the first question one might as is "How do I solve this puzzle?" However, there is perhaps an even more natural question that we need to answer first: "Is it even possible to solve this puzzle?"

We will paraphrase this question a little bit in order to think about a slightly more tangible question. Notice that if it is possible for us to solve this puzzle, then we can find a sequence of moves in which we slide the tiles to get from our starting configuration to the identity configuration. Each of these moves individually can be reversed (the opposite of "slide some tile into the empty space" is "slide that tile right back where it came from"), so we can see that if there is a sequence of moves that gets us from the starting configuration to the identity configuration, then there is **also** a sequence of moves that will take us from the identity configuration back to this starting configuration.

So we can now rephrase our question "Is it possible to solve this puzzle?" into "Given a configuration of the puzzle, does there exist a sequence of moves that can take me from the identity configuration to this configuration?" While this paraphrasing certainly seems more wordy, it is actually an easier question to answer. We will later develop a tool from Group Theory which will help us answer this question, but let's first look at some examples of a smaller case of this puzzle.

For a 2 by 2 version of the puzzle, the solved configuration looks like this:

1	2
3	

Now, you can perhaps easily convince yourself that the following configuration is able to be solved:

2	3
1	

while you can (maybe a little less easily) convince yourself that the following configuration is not able to be solved:

2	1
3	

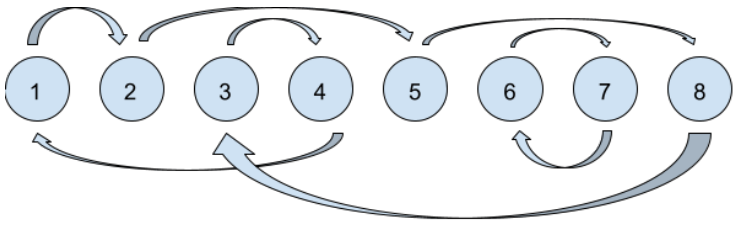
So it seems the answer to our important question about solvability is "sometimes yes; sometimes no", so now our goal is to try and develop the rules for when a configuration of this puzzle is or is not solvable.

2 The Symmetric Group

If we have a collection of n objects, say the numbers $\{1, 2, \ldots, n\}$, then a *permutation* of this set is a way to rearrange the set into a particular order. In other words, the set of permutations on this set is the same as the set of invertible maps[1] from this set to itself. This set of permutations actually forms a mathematical group (which we call the *Symmetric Group*, denoted S_n). This all sounds a bit abstract, so perhaps some examples of these permutations will help clear things up.

Note: Throughout, we shall use lower case Greek letters to denote permutations. These include σ, or sigma; τ, or tau; and ρ, or rho (pronounced like "row", as in "row, row, row your boat").

Firstly, we can see a permutation as both a way to rearrange a set of numbers *or* as a map from the set of numbers to itself. For example, the map that rearranges the numbers $\{1, 2, 3, 4, 5, 6, 7, 8\}$ in the following way:



can be seen as a map $\{1, 2, 3, 4, 5, 6, 7, 8\} \to \{1, 2, 3, 4, 5, 6, 7, 8\}$ that sends

$$1 \mapsto 2, \quad 2 \mapsto 5, \quad 3 \mapsto 4, \quad 4 \mapsto 1, \quad 5 \mapsto 8, \quad 6 \mapsto 7, \quad 7 \mapsto 6, \quad 8 \mapsto 3.$$

[1] By "invertible maps", here we mean functions from $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ where every number is included exactly once as an input and exactly once as an output.

Let us consider the set $\{1, 2, 3\}$, and the map σ that sends $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. We may also write this in something that resembles function notation, $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$, or we can write this in what's known at *two-line* notation:

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

We have another permutation which we can call τ, which sends $1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2$. Then, τ can also be written:

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Exercise 2.1. Verify that σ and τ are actually permutations (i.e., invertible maps). In other words, what is the inverse map[2] for each of these permutations? Write these inverse permutations

Now as an example of something that is **not** a permutation, we can look at the map ρ, which sends $1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 2$, or in two-line notation:

$$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \end{pmatrix}$$

Exercise 2.2. Why is ρ not a permutation?

[2]Here, the *inverse map* is the function that "reverses all of the arrows" of the original map. So if the permutation σ sends $a \mapsto b$, then the inverse map σ^{-1} sends $b \mapsto a$.

Now we notice that the first line of this two-line notation is always the same—just each of the numbers from 1 to n in order—so this is a bit redundant and sometimes cumbersome. Since we as mathematicians can sometimes be pretty lazy, very often instead use a more descriptive and concise notation known as *cycle* notation. In this notation, instead of looking at the map as a whole, we consider it in terms of the "closed loops" it creates.

After identifying the closed loops of a permutation, we write these loops as cycles by writing the elements next to each other in the order they appear in the loop. Also, if a permutation sends an element to itself (we call this a fixed point), then we can write it in a cycle by itself, but we can also just omit it from the cycle notation and understand that any element that isn't part of the cycle notation is a fixed point.

For example, with our permutation σ above, we have the closed loop $1 \mapsto 2 \mapsto 3 \mapsto 1$, so we write this as the cycle $(1\,2\,3)$. A couple of notes on cycle notation: First, we close off each cycle once we get back to the point we started at so we can avoid writing the same element twice. Second, we can "start" the cycle at any point in the loop (for example, the loop $(1\,2\,3)$ is the same as $(2\,3\,1)$), so by convention we usually write cycles starting with the smallest number in the loop.

Exercise 2.3. What is the cycle notation for $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$?

Exercise 2.4. As a larger example, let's look at an element of S_6, a permutation on the set $\{1, 2, \ldots, 6\}$ given in two-line notation by

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}$$

This has two closed loops $1 \mapsto 3 \mapsto 4 \mapsto 6 \mapsto 1$ and $2 \mapsto 5 \mapsto 2$. How can we write this in cycle notation?

One last property of permutations we'll discuss is the notion of the *parity* of a permutation. The parity of a permutation is a number (either 1 or -1) which describes, among other things, the number of transpositions (2-cycles) needed to build a permutation. If a permutation has parity -1, we call it an *odd* permutation and if it has parity 1, we call it an *even* permutation.

We can use the cycle notation of a permutation to compute its parity using two facts. First, if σ is a cycle of length ℓ, then the parity of σ, which we'll call $p(\sigma)$ is

$$p(\sigma) = (-1)^{\ell+1}$$

(Note that this makes our use of the words "even" and "odd" a little confusing because cycles with even length are odd permutations and cycles with even length are odd permutations). The second fact is that the parity of a product of two permutations[3] is the product of their parities.

For example, if $\sigma = \sigma_1\sigma_2 \dots \sigma_k$, then the parity

$$p(\sigma) = p(\sigma_1)p(\sigma_2)\cdots p(\sigma_k).$$

Therefore, looking at our example from earlier where $\rho = (1\,3\,4\,6)(2\,5)$, we have that $p(\rho) = (-1)^5(-1)^3 = 1$.

Exercise 2.5. Write the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 1 & 4 & 7 & 6 & 8 \end{pmatrix}$ in cycle notation and find its parity.

Exercise 2.6. Write the permutation $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 8 & 7 & 3 & 2 & 4 & 5 \end{pmatrix}$ in cycle notation and find its parity.

[3]When we write two permutations next to each other like (1364)(25), it looks like we're multiplying two things together. This really acts as a sort of "function composition" where this means "first do the permutation (25) that swaps 2 and 5, and then do the permutation (1364) that rotates $1 \mapsto 3 \mapsto 6 \mapsto 4 \mapsto 1$.

Exercise 2.7. There are 6 elements of the Symmetric Group on 3 elements, S_3:

- $(1)(2)(3)$
- $(1\,2\,3)$
- $(1\,2)(3)$
- $(1)(2\,3)$
- $(1\,3\,2)$
- $(1\,3)(2)$

Identify which are even permutations and which are odd permutations. Can you say something about the parity of a permutation based on the number of even-length and odd-length cycles it has?

Exercise 2.8. What is the parity of the product of two even permutations? Of two odd permutations? Of one even and one odd permutation? Do these rules of combining even and odd permutations look like something more familiar to us?

The rest of this document will act as something of a "Choose-Your-Own-Adventure". The following sections can really be done in any order you like, and you can skip around if you so choose. If you would like to see how these permutations relate to the solvability of the Fifteen Puzzle, skip to Section 3. If you would like to explore actually solving the puzzle, skip to Section 4. If you would like to learn more background about permutations and the Symmetric Group, skip to Section 5 (this one may be the most challenging and unfamiliar).

3 The Fifteen Puzzle

Now we go back to attempt to answer our important question about solvability of the Fifteen Puzzle, but first we need a way to translate from a particular configuration of our board to a particular permutation. We'll label every tile with its corresponding number and then label the empty slot with one greater than the largest number (for the 2 by 2 case, the empty slot will be labelled 4, for the 4 by 4 case, it will be labelled 16). Then, for a particular configuration, we'll define σ for each number i by $\sigma(i) =$"the number of the space that the i tile is in."

For example, the board

7	11	9	10
14	13	2	3
1	6	15	8
12	4	5	

will correspond to the permutation

$$\sigma = (1\ 9\ 3\ 8\ 12\ 13\ 6\ 10\ 4\ 14\ 5\ 15\ 11\ 2\ 7),$$

and the board

1	2	3	4
5	7	6	8
9	10	11	12
13	14	15	

will correspond to the permutation $\sigma = (6\ 7)$

Exercise 3.1. There are 6 possible 2 by 2 boards with the empty spot in the lower left:

1	2
3	

1	3
2	

2	1
3	

3	2
1	

2	3
1	

3	1
2	

For each of these boards, identify the permutation associated to the board and whether or not this board is solvable.

Exercise 3.2. Do you notice any correlation between solvability of the puzzle and the permutation?

Exercise 3.3. Based on what you found in the previous exercise, predict whether the following boards are solvable or not:

7	11	9	10
14	13	2	3
1	6	15	8
12	4	5	

1	2	3	4
5	7	6	8
9	10	11	12
13	14	15	

Exercise 3.4. The following are some interesting configurations of the Fifteen Puzzle. For each configuration, write it as a permutation of the "solved" board. Which of these permutations are odd? Which ones are even? Which ones do you think are solvable?

Exercise 3.5. In the game, we can't just swap *any* two tiles. We can only swap the blank space with a tile right next to it. Suppose we do a sequence of moves and the blank space starts and ends in the bottom right corner.

a) If the sequence contains 5 moves that move the blank space to the left by one, how many moves in the sequence move the blank space to the right by one?

b) If the sequence contains 7 moves that move the blank space up by one, how many moves in the sequence move the blank space down by one?

Exercise 3.6. If a sequence of moves starts and ends with the blank space in the bottom right square, what can we say about the total number of moves in the sequence?

Exercise 3.7. If a Fifteen Puzzle configuration has the blank space in the bottom right corner, what can we say about the permutation associated to that configuration. (Think about what we said about the number of transpositions in a particular permutation)

Exercise 3.8. Why does this mean the odd permutations are not solvable?

4 Solving the Fifteen Puzzle

Exercise 4.1. Suppose we just have a 2-by-2 slide puzzle in an unsolved configuration. Here are some examples:

2	3
1	

3	1
2	

What moves can we do to solve these puzzles?

Exercise 4.2. Suppose now we add an extra column and have a 2-by-3 slide puzzle whose solution is

1	2	3
4	5	

Here is an example of an unsolved one:

2	4	3
1	5	

If we can get the numbers 1 and 4 in the correct positions, how can we then put $2, 3$, and 5 in the correct positions? Can you figure out how to get 1 and 4 into the correct positions?

Exercise 4.3. Suppose we have a 3-by-3 slide puzzle whose solution is

1	2	3
4	5	6
7	8	

Here is an example of an unsolved one:

1	6	7
8	4	2
3	5	

Which tiles should I make sure I can put into place in order to reduce this problem to a previously solved case?

Exercise 4.4. Now given any 4-by-4 Fifteen puzzle with the solution

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

can you develop a strategy for which tiles to get into their places in order to keep reducing our puzzle to previously-solved smaller cases?

5 Symmetric Groups, Revisited

So far, all of the permutations we have written in cycle notation look like the product of *disjoint* cycles, meaning none of the cycles we write have any elements in common. Here we will explore how to write products of cycles where some of these cycles share elements.

Perhaps the most surprising thing is that when we compose/multiply permutations, we do so right-to-left. So for example, when we write the product (1234)(325), we mean "do the permutation (253) that sends

$$1 \mapsto 1, \quad 2 \mapsto 5, \quad 3 \mapsto 2, \quad 4 \mapsto 4, \quad 5 \mapsto 3$$

and then do the permutation (1234) that sends

$$1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 4, \quad 4 \mapsto 1, 5 \mapsto 5."$$

This composition is computed as

$$1 \overset{(325)}{\mapsto} 1 \overset{(1234)}{\mapsto} 2, \quad 2 \overset{(325)}{\mapsto} 5 \overset{(1234)}{\mapsto} 5, \quad 3 \overset{(325)}{\mapsto} 2 \overset{(1234)}{\mapsto} 3, \quad 4 \overset{(325)}{\mapsto} 4 \overset{(1234)}{\mapsto} 1, \quad 5 \overset{(325)}{\mapsto} 3 \overset{(1234)}{\mapsto} 4,$$

simplifying to

$$1 \mapsto 2, \quad 2 \mapsto 5, \quad 3 \mapsto 3, \quad 4 \mapsto 1, \quad 5 \mapsto 4,$$

which is (in disjoint cycle notation) the permutation (1254)(3).

Exercise 5.1. We can write the 3-cycle (132) as the product of transpositions/2-cycles (32)(21). Check that (132) is indeed the same permutation as (32)(21). How would you write (123) as a product of transpositions?

Exercise 5.2. How would you write the 4-cycle (4268) as a product of transpositions? (There may be multiple ways.)

Exercise 5.3. If we can write a single cycle (like (132), for example) as a product of transpositions, then the transpositions cannot be disjoint. In other words, two or more of the transpositions must move the same set element. Why is this the case?

Exercise 5.4. One of the possible ways of writing (4268) is (42)(26)(68). What do you notice about each of the transpositions?

Exercise 5.5. In general, how would you write a k-cycle $\sigma = (i_1...i_k)$, where each i_j, $1 \leq j \leq k$ is some integer, as a product of transpositions? What do you notice about the number of transpositions you used? In particular, this should be able to tell us something about why we consider even-length cycles to be odd permutations and odd-length cycles to be even permutations.

Exercise 5.6. Consider now the transposition (37). How would you write this as a product of adjacent transpositions? In other words, how would you write (37) only using the transpositions $(34), (45), (56), (67)$?

Exercise 5.7. Generalize the last problem to the transposition (ab), where a and b are integers with $a < b$.

Exercise 5.8. Recall that $(4625) = (42)(26)(68)$. How would you write (4625) as a product of adjacent transpositions, i.e. transpositions of the form $(i, i+1)$?

Exercise 5.9. Generalize this to the cycle $\sigma = (i_1...i_k)$, i.e. write the cycle σ as a product of adjacent transpositions.

Exercise 5.10. Show that (132) and $(12)(13)$ are the same permutation, giving another way to write the 3-cycle as a product of transpositions.

Exercise 5.11. How would you express the permutation (528397) in this way, i.e. as a product $(5i_1)(5i_2)...(5i_k)$? What should the i_j be?

Now consider the general case: how would you express $\sigma = (i_1...i_k)$ as a product of transpositions, where each transposition acts on a common element?