Lecture 8: Permutations: A_n and 3-Cycles

Contents

In this lecture we focus our attention on the set of even permutations, A_n, and show every even permutation can be written as a product of 3-cycles.

8.1 Swap Variation: A Challenge

Consider the following variation of Swap:

Variation: Legal move is to pick any 3 boxes and cycle their contents either to the left or right.

Using only these legal moves, try the following challenges.

Challenge 1: Solve the following puzzle:

1	2	3	4	5	6	7	8	9	10
4	8	2	6	5	1	3	7	10	9

Challenge 2: Solve the following puzzle:

1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	10	9

8.2 The Alternating Group A_n

In Lecture 6 we discovered there are two types of permutations: even and odd. We will denote the **set of all even permutations** by A_n, and the **set of all odd permutations** by O_n. Since every permutation is either odd or even, and no permutation is both, it follows that

$$S_n = A_n \cup O_n, \qquad \text{where } A_n \cap O_n = \emptyset.$$

There is one difference between these two sets which will be important for us, and this has to do with how each of the sets behaves under composition.

> The set A_n of even permutations is closed under composition, closed under taking inverses, and contains the identity. The set O_n of odd permutations is closed under taking inverses, but definitely not closed under composition, nor does it contain the identity. In fact, the composition of an two permutations in O_n is always in A_n.

When we say that A_n (or, in general, *any* subset of B of S_n) is **closed under composition**, we mean that for any $\alpha, \beta \in A_n$ (or in B) the composition $\alpha\beta \in A_n$ (in B). Similarly, by **closed under taking inverses** we mean that for any $\alpha \in A_n$ (or in B) the inverse permutation α^{-1} is also in A_n (in B)

Let's check why our statements about A_n and O_n are true. The product of any two even permutations is another even permutation so A_n is closed under composition. The identity permutation is even and therefore in A_n. For any permutation $\alpha \in A_n$, it's inverse α^{-1} is also even, since once way to express α^{-1} as a product of transpositions is to just write the ones expressing α in reverse order. So if an even number were used to express α then an even number can be used to express α^{-1}. Similarly, if $\beta \in O_n$ then $\beta^{-1} \in O_n$. The product of two odd permutations gives a permutation that can be expressed in terms of an *odd* + *odd* = *even* number of transpositions, and therefore is an even permutation.

This distinction between A_n and O_n will makes A_n a much more important object to study. Why? Well, to answer this we go back to the properties of S_n.

In Lecture 3, we defined the set of all permutations to be the *Symmetric Group*, S_n. We listed various properties this set has, but most notably it has the following four properties regarding composition:

(a) **Closure.** The product of two elements $\alpha, \beta \in S_n$ is another element $\alpha\beta \in S_n$.[1]

(b) **Associativity.** Permutation composition is associative: $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

(c) **Identity.** The *identity* (or "do nothing") permutation ε is in S_n. It has the property that $\varepsilon\alpha = \varepsilon\alpha = \alpha$ for all $\alpha \in S_n$.

(d) **Inverses.** Every $\alpha \in S_n$ has an *inverse* in S_n denoted by α^{-1}. The defining property of an inverse is $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \varepsilon$.

If we look back at all the computations we've done with permutations we see that we are making extensive use of these properties, whether we are conscious of it or not. For example, the cancellation property: $\alpha\beta = \alpha\gamma$ implies $\beta = \gamma$, and $\beta\alpha = \gamma\alpha$ implies $\beta = \gamma$, is a direct consequence of these four properties. Look back at the proof of it in Lecture 3. This means that any set of objects, equipped with an operation that combines two to produce a third, and the operation satisfies these four properties, also has the cancellation property. For example, $\mathbb{R}$ under the operation of addition, +, satisfies these four properties (identity is 0), so it must also have the cancellation property. The set of invertible 2×2 matrices, under matrix multiplication, satisfies these four properties, so it must also have the cancellation property. In a sense, we have described the "important" properties of S_n.

A set A that comes equipped with an operation to combine pairs of elements (add/multiply/compose) such that A is *closed* under the operation, the operation is *associative*, there is an *identity* in A, and

[1] the convention of these notes is to compose permutations from left-to-right,

inverses exist in A, is called a **group**. Our explorations into permutations puzzles will essentially consist of considering the set of all legal move sequences, call this set M, and noticing that this set is a subset of S_n which is also a group. (Composition of legal moves is a legal move, composition is associative, there is a "do-nothing" move, and for each move there is an way to "undo" it.) Therefore to each permutation puzzle we can associate a group M of legal move sequences. The question is then: Are we able to understand the group M? In order to do this, we'll need to build up our stock of examples of groups.

What we've shown above is that A_n is a group, whereas O_n is not. O_n fails to contain the identity, nor is it closed under composition. A_n is an important family of groups, and in particular A_5 has great historical significance. The letter "A" in its name comes from the word "alternating", which reflects some properties that were important when these groups were first studied.

Definition 8.1 (Alternating Group of Degree n) *The set of even permutations of S_n is denoted by A_n, and is called the* ***alternating group of degree n****:*

$$A_n = \{\alpha \in S_n : \alpha \textit{ is an even permutation}\}$$

We will sometimes refer to A_n as the *set of even permutations*. As a first step in investigating A_n, lets show it contains exactly half the elements of S_n.

Theorem 8.1 (Cardinality of A_n) $|A_n| = |O_n| = \dfrac{n!}{2}$, *for* $n \geq 2$.

Proof: To see this we will pair up all the even permutations α with odd permutations $(1,2)\alpha$, to observe there are equal numbers of each.

Consider the set of all elements in S_n of the form $(1,2)\alpha$ where $\alpha \in A_n$, and denote this set by $(1,2)A_n$:

$$(1,2)A_n = \{(1,2)\alpha : \alpha \in A_n\}$$

Observe that $(1,2)A_n \subset O_n$, since extending an even permutation by a transposition is an odd permutation. On the other hand, for $\beta \in O_n$ we have $(1,2)\beta \in A_n$ and so $\beta = (1,2)(1,2)\beta \in (1,2)A_n$. Since β was just any element of O_n this means, $O_n \subset (1,2)A_n$. It follows that $O_n = (1,2)A_n$.

Next we note that $(1,2)A_n$ and A_n have exactly the same number of elements. To see this, we just observe that the function $\phi : A_n \to (1,2)A_n$ defined by $\phi(\alpha) = (1,2)\alpha$ is a bijection. (See exercise 11.)

Therefore $|A_n| = |O_n|$ and $|A_n| + |O_n| = |S_n|$. Since $|S_n| = n!$ it follows that $A_n = O_n = \frac{n!}{2}$. $\square$

Example 8.1 *List the elements of A_4.*

These are the permutations in S_4 which are even. The most straightforward way to list elements is to do it in disjoint cycle form, so we'll begin with the identity:

$$\varepsilon.$$

Next, we list elements involving cycles of length at most 2. And since we want even permutations we don't included single transpositions:

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

Next we can list 3-cycles:

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

This is all the elements of A_4, and there are 12 as predicted by Theorem 8.1.

8.3 Products of 3-cycles

The fact that every permutation in S_n can be expresses as a product of 2-cycles, is something we have used quite a bit. There is a similar result for the even permutations A_n and 3-cycles.

Theorem 8.2 *Every permutation in A_n, for $n \geq 3$, can be expressed as a product of 3 cycles.*

Proof: Suppose α is an even permutation, then we can express it as the product of an even number of 2-cycles:

$$\alpha = \tau_1 \tau_2 \cdots \tau_{2k-1} \tau_{2k}.$$

We'll group together adjacent pairs of 2-cycles as follows:

$$\alpha = (\tau_1 \tau_2)(\tau_3 \tau_4) \cdots (\tau_{2k-1} \tau_{2k}).$$

It suffices to show that a product of two transpositions can either be dropped from the expression or be expressed as a product of 3-cycles, without changing the the value of the expression.

Each product $\tau_i \tau_{i+1}$ can be expressed in one of the following ways as shown on the left, depending on whether the transpositions move two things in common, one thing in common, of nothing in common:

$$(a,b)(a,b) = \varepsilon$$
$$(a,b)(a,c) = (a,b,c)$$
$$(a,b)(c,d) = (a,b,c)(a,d,c)$$

If the first case occurs we may delete $\tau_i \tau_{i+1}$ in the original product. In the other two cases we replace $\tau_i \tau_{i+1}$ with what appears on the right to obtain a new product of 3-cycles. □

Example 8.2 *Express the even permutation $\alpha = (1,6,4)(2,3,7,8)(9,10)$ as a product of 3-cycles.*

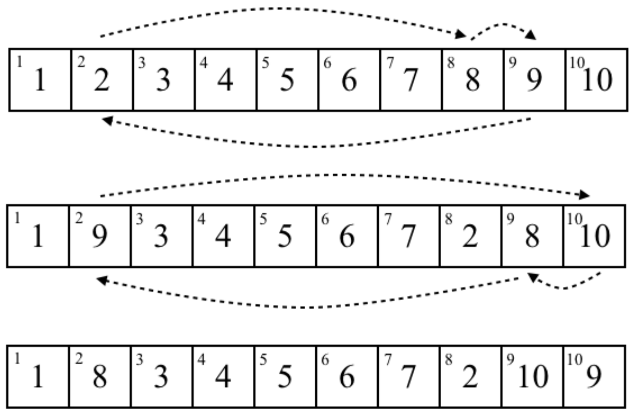
To do this the first thing we do is express it as a product of transpositions:

$$\alpha = (1,6)(1,4)(2,3)(2,7)(2,8)(9,10)$$

Then we group adjacent transpositions and express each in terms of 3-cycles.

$$(1,6)(1,4) = (1,6,4)$$
$$(2,3)(2,7) = (2,3,7)$$
$$(2,8)(9,10) = (2,8,9)(2,10,9)$$

It may seem mysterious how we obtained the last one. The following simple game of Swap shows how we can express $(2,8)(9,10)$ as the product of two 3-cycles.



In general, this is precisely the result we used in the proof of the theorem. The way we came up with it there was to look at a simple game of Swap on four objects $a|b|c|d$. To swap a with b and c with d we can first cycle abc to the right: $c|a|b|d$. Then we can cycle objects in positions acd to the left: $b|a|d|c$.

Now we can put everything back together to get:

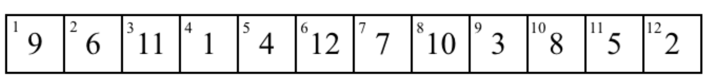
$$\alpha = (1, 6, 4)(2, 3, 7)(2, 8, 9)(2, 10, 9).$$

8.4 Variations of Swap: Revisited

Let's go back to the variation of Swap in Section 8.1.

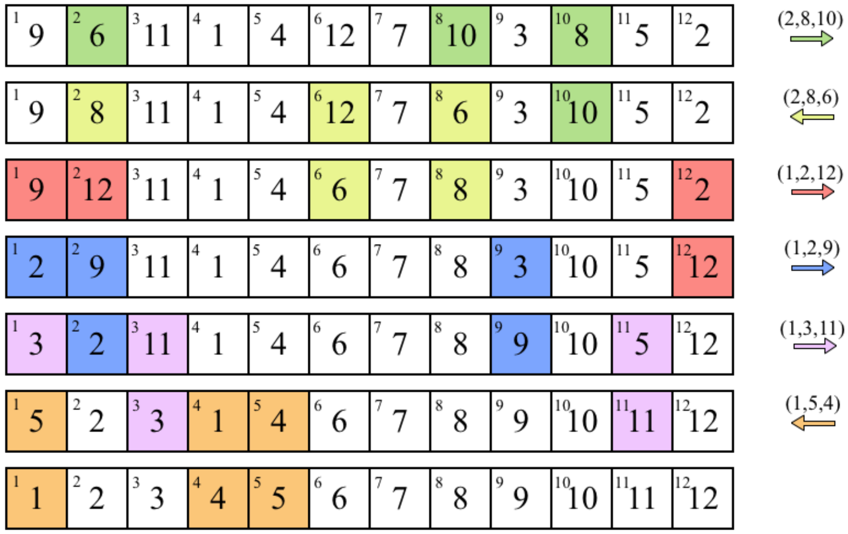
Variation: Legal move is to pick any 3 boxes and cycle their contents either to the left or right.

For example, suppose the puzzle started in the following position:



The corresponding permutation is $\alpha = (1, 4, 5, 11, 3, 9)(2, 12, 6)(8, 10)$.

We can solve the puzzle as follows. In each line the shaded boxes represent our choice of 3 boxes, and the arrow on the right indicates which direction the contents are being moved. We also summarize the move by writing the corresponding 3-cycle above the arrow.



In term of permutations this move sequence tells us:

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

or in other words,

$$\begin{aligned}\alpha &= [(2,8,10)(2,8,6)(1,2,12)(1,2,9)(1,3,11)(1,5,4)]^{-1}\\ &= (1,4,5)(1,11,3)(1,9,2)(1,12,2)(2,6,8)(2,10,8).\end{aligned}$$

That is, considering α as a starting position for this variation of Swap, solving the puzzle is equivalent to expressing α as a product of 3-cycles. Since we know only even permutations are expressible as products of 3-cycles this give us a very simple solvability condition for this variation of Swap.

Corollary 8.1 (Solvability of Swap Variation) *The Swap puzzle, where the legal moves consist of 3-cycles on any three boxes, is solvable only when the starting position is an even permutation. In other words, only even permutations can be obtained in this variation of Swap.*

To see this solvability condition in action, consider the following scramble of Swap.

1	2	3	4	5	6
2	6	4	1	3	5

Try solving it using only 3-cycles.

You would very quickly realize it is a difficult task. It is possible to get all but two numbers back into their home positions. In fact, this position corresponds to the permutation $(1,4,3,5,6,2)$ which is a 6-cycle, and therefore an odd permutation. Therefore, by Theorem 8.1 no matter how long we play with the puzzle it we don't have a hope of solving it. It is simply impossible!

Looking back at Section 8.1 we see that the permutation in Challenge 1 is $(1,6,4)(2,3,7,8)(9,10)$ which is even and hence solvable, whereas the permutation in Challenge 2 is $(9,10)$ which is odd, and therefore not solvable. Just knowing Challenge 1 is solvable doesn't actually answer the question, we were actually asked to solve the puzzle. This is equivalent to expressing $(1,6,4)(2,3,7,8)(9,10)$ as a product of 3-cycles, which we've already done in Example 8.2. there we found $(1,6,4)(2,3,7,8)(9,10) = (1,6,4)(2,3,7)(2,8,9)(2,10,9)$. So applying the inverse of this permutation: $(2,9,10)(2,9,8)(2,7,3)(1,4,6)$ will solve the puzzle. On the other hand, knowing the puzzle in Challenge 2 is not solvable means we can abandon playing with it, since there is not way to solve it.

8.5 Exercises

1. Given an example of an element in A_7 which contains a 4-cycle. Give an example of an element in A_{10} which contains at least one 3-cycle, and at least one 4-cycle.

2. Demonstrate the truth of Theorem 8.2 by expressing these even permutations as products of 3-cycles.

   (a) $\alpha = (1,2)(1,3)$
   (b) $\beta = (1,2)(3,4)$
   (c) $\gamma = (1,2,3,4,5,6)(3,4,5)(2,5)(1,4)(5,2)$
   (d) $\delta = (1,2)(2,3)(4,5)(1,3)(6,7)(6,8)(9,10)(11,12)$
   (e) $\sigma = (1,2,3,4)(2,3,4,5)(4,5,6,7)(8,9)$

3. **Expressing odd permutations in terms of 3-cycles and one transposition.**
   (a) Show that all odd permutations in S_n can be expressed using exactly one transposition together with zero or more 3-cycles.
   (b) Demonstrate the truth of this claim by expressing these odd permutations with a single transposition and 3-cycles.

   (i) $\alpha = (1,2,3,4,5,6)$
   (ii) $\beta = (1,2,3,4)(5,6,7)(8,9,10)$
   (iii) $\gamma = (2,5,3,7,6)(3,5,8,4)(6,8,2,1,9)$

4. Using the solvability condition for the variation of Swap we considered in this section (Corollary 8.1), determine whether each of the following scrambles are solvable. For the ones that are solvable, find a sequence of moves that solve the puzzle.

   (a)

1	2	3	4	5	6
3	5	1	6	4	2

   (b)

1	2	3	4	5	6	7	8	9	10
6	9	5	2	1	8	10	3	4	7

   (c)

1	2	3	4	5	6	7	8	9	10
2	9	1	10	6	7	3	5	8	4

   (d)

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

5. What are the possible orders for permutations in A_6? What about A_7?

6. Show that A_5 contains no element of order 15.

7. What is the maximum order of any element in A_{10}?

8. Compute the order of each permutation in A_4. What arithmetic relationship do these orders have with he cardinality of A_4.

9. How many elements of order 5 are there in A_6.

10. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.

11. Show that the function $\phi : A_n \to (1,2)A_n$ defined by $\phi(\alpha) = (1,2)\alpha$ is a bijection. (This result is used in the proof of Theorem 8.1.)

12. **Products of 4-cycles? 5-cycles?** All permutations in S_n are expressible using transpositions, and all permutations in A_n are expressible using 3-cycles, provided $n \geq 3$. Stating this another way, this says that you get all permutations by taking all possible products of 2-cycles, and similarly you get all the even permutations by taking all possible products of 3-cycles. What do you get when you take all possible products of 4-cycles? Or 5-cycles. Or k-cycles? Explore this question and see what you can discover. Note of course that we must assume $n \geq k$ before we can talk about k-cycles in S_n.