On an open problem of the symmetric group

Dana C. Ernst

Plymouth State University
Mathematics Department

http://oz.plymouth.edu/~dcernst

PSU Mathematics Seminar
April 28, 2010

Goal

What is mathematical research?

Research in mathematics takes many forms, but one common theme is that the research seeks to answer an open question concerning some collection of mathematical objects.

The goal of this talk will be to introduce you to one of the many open questions in mathematics:

Open Question

How many commutation classes does the longest element in the symmetric group have?

We will review the basics of the symmetric group and introduce all of the necessary terminology, so that we can understand this question.

Groups

Groups are fundamental objects in mathematics.

Intuitive definition

Start with a static collection of objects (a set), throw in a method for combining two objects together (a binary operation) so that it satisfies some reasonable requirements (associative, identity, and inverses), and you've got yourself a group.

Whereas sets just sit there, groups have the ability for elements to interact with each other. It is this key idea that gives birth to symmetry and the beauty of group theory.

The extremely vague fact

All groups "do" something. Every element of a group can be thought of as an "action."

If I want to understand a group, I think about what all of the actions are. Combining two elements in a group together means "do the first action, then apply the second action to the result."

OK, we need a toy to play with.

Definition

The symmetric group S_n is the collection of bijections from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$ where the operation is function composition (left $\leftarrow$ right).

What do elements of S_n "do"? Each element rearranges an arrangement of n objects; called a permutation.

Let's play with S_5. I need 5 volunteers!

Things to think about:

- What is the identity permutation?
- Given a permutation, what is its inverse?
- How do you compose two permutations?

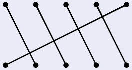
Permutation diagrams

One way of representing elements from S_n is with permutation diagrams, which are best illustrated with examples.

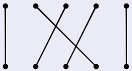
Example

Here are some examples of permutation diagrams in S_5.

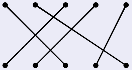
$\alpha =$



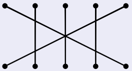
$\beta =$



$\sigma =$



$\gamma =$



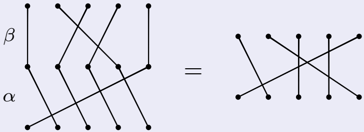
Permutation diagrams (continued)

Let's try multiplying.

Example

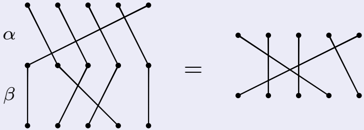
Let α and β be as on previous slide. Then

$\alpha\beta =$



But on the other hand

$\beta\alpha =$

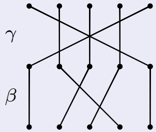
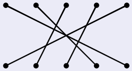


We see that products of permutations do not necessarily commute (order matters).

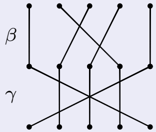
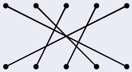
However, sometimes permutations do commute.

Example

Let β and γ be as before. Then

$\beta\gamma =$  $=$ 

But

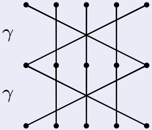
$\gamma\beta =$  $=$ 

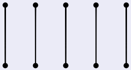
Notice that these result in the same diagram. So, β and γ commute.

Let's do one more example.

Example

Let γ be as before. Then

$\gamma\gamma =$ 

$=$ 

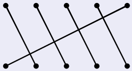
The rightmost diagram is the identity in S_5 (it's the "do nothing action"). Since $\gamma\gamma$ is equal to the identity, γ must be its own inverse.

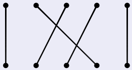
Cycle notation

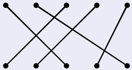
We need a more efficient way of encoding information. One way to do this is using cycle notation.

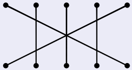
Example

Consider α, β, σ, and γ in S_5 as in the previous examples.

$\alpha =$  $= (1\ 2\ 3\ 4\ 5)$

$\beta =$  $= (2\ 4\ 3)$

$\sigma =$  $= (1\ 3)(2\ 5\ 4)$

$\gamma =$  $= (1\ 5)$

Let's try multiplying cycles.

Example

Let α and β be as before. Then

$$\alpha\beta = (1\ 2\ 3\ 4\ 5)(2\ 4\ 3) = (1\ 2\ 5).$$

On the other hand,

$$\beta\alpha = (2\ 4\ 3)(1\ 2\ 3\ 4\ 5) = (1\ 4\ 5).$$

We could easily check that the products above equal the diagrams that we found earlier. Again, we see that products of permutations do not necessarily commute.

Example

Let β and γ be as before. Then

$$\beta\gamma = (2\ 4\ 3)(1\ 5) = (1\ 5)(2\ 4\ 3) = \gamma\beta.$$

We saw earlier that β and γ commute with each other.

Cycle notation (continued)

We've stumbled upon the following general fact.

Theorem

Products of disjoint cycles commute.

Let's do one last example of multiplication involving cycles.

Example

As before, let $\gamma = (1\ 5)$. Then

$$\gamma\gamma = (1\ 5)(1\ 5) = (1) = \text{identity}.$$

Here's another general fact.

Theorem

2-cycles have order 2. That is, a 2-cycle is its own inverse.

The adjacent 2-cycles

Some of the 2-cycles play a key role in what I would like to say today.

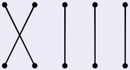
Definition

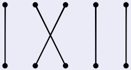
In S_n, the adjacent 2-cycles are the cycles

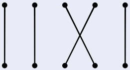
$$(1\ 2), (2\ 3), (3\ 4), \ldots, (n-2\ \ n-1), (n-1\ \ n).$$

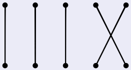
Example

The adjacent 2-cycles in S_5 are $(1\ 2), (2\ 3), (3\ 4)$, and $(4\ 5)$.

$(1\ 2) =$ 

$(2\ 3) =$ 

$(3\ 4) =$ 

$(4\ 5) =$ 

The adjacent 2-cycles (continued)

What's so special about the adjacent 2-cycles?

Theorem

Every element in S_n can be written as a product of the adjacent 2-cycles. That is, the adjacent 2-cycles generate S_n.

Unfortunately, we don't have time to discuss one of the algorithms for turning a permutation into a product of the adjacent 2-cycles.

However, it is important to note that there are potentially many different ways to express a given permutation as a product of adjacent 2-cycles.

Example

Consider the following products in S_4:

$$(1\ 2)(3\ 4)(2\ 3)(1\ 2)(2\ 3) \quad \text{and} \quad (3\ 4)(2\ 3)(1\ 2).$$

It turns out that these are both expressions for the element $(1\ 4\ 3\ 2)$. This is easily verified by just multiplying out each expression.

Relations of the symmetric group

It will be useful for us to have methods for converting one expression into another. It turns out that we only need three "tools."

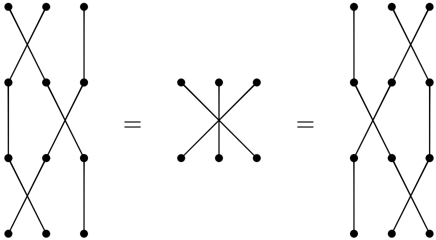
Theorem

The symmetric group S_n is generated by the adjacent 2-cycles subject only to the following relations.

1. $(i\ i+1)^2 = (1)$ (2-cycles have order two)
2. $(i\ i+1)(j\ j+1) = (j\ j+1)(i\ i+1)$, where $|i-j| > 1$ (disjoint cycles commute)
3. $(i\ i+1)(i+1\ i+2)(i\ i+1) = (i+1\ i+2)(i\ i+1)(i+1\ i+2)$ (braid relations)

What this theorem really means is that all the symmetric group needs is the adjacent 2-cycles and these 3 rules for manipulating products of them.

We've already seen that 2-cycles have order 2 and that disjoint cycles commute. How about the braid relations?



Examples involving the relations

Let's return to the previous example.

Example

We see that

$$\begin{aligned}(1\ 2)(3\ 4)(2\ 3)(1\ 2)(2\ 3) &= (1\ 2)(3\ 4)(1\ 2)(2\ 3)(1\ 2)\\ &= (1\ 2)(3\ 4)(1\ 2)(2\ 3)(1\ 2)\\ &= (3\ 4)(1\ 2)(1\ 2)(2\ 3)(1\ 2)\\ &= (3\ 4)(1\ 2)(1\ 2)(2\ 3)(1\ 2)\\ &= (3\ 4)(2\ 3)(1\ 2)\end{aligned}$$

Comments

1. If we express a permutation as a product of adjacent 2-cycles in the most efficient way possible, then we call the expression a reduced expression.
2. There may be many different reduced expressions for a given permutation, but all of them can be written in terms of the same number of adjacent 2-cycles occurring in the product (called the length).

Examples involving the relations (continued)

Example

We've already seen that

$$(1\ 2)(3\ 4)(2\ 3)(1\ 2)(2\ 3) \quad \text{and} \quad (3\ 4)(2\ 3)(1\ 2)$$

represent the same permutation. The first of these expressions is not reduced, but the second one is and has length 3.

It turns out that $(3\ 4)(2\ 3)(1\ 2)$ is the only reduced expression for $(1\ 4\ 3\ 2)$.

Theorem (Matsumoto)

Given two reduced expressions for the same permutation, we can obtain one reduced expression from the other by commuting disjoint cycles and applying braid relations.

Let's take a look at a more complicated example.

Example

The set of all reduced expressions for (1 3 5 4) in S_5 is listed below:

(1 2)(2 3)(1 2)(4 5)(3 4)	(1 2)(2 3)(4 5)(1 2)(3 4)	(1 2)(4 5)(2 3)(1 2)(3 4)
(1 2)(2 3)(4 5)(3 4)(1 2)	(1 2)(4 5)(2 3)(3 4)(1 2)	(4 5)(1 2)(2 3)(3 4)(1 2)
(4 5)(1 2)(2 3)(1 2)(3 4)	(2 3)(1 2)(2 3)(4 5)(3 4)	(2 3)(1 2)(4 5)(2 3)(3 4)
(2 3)(4 5)(1 2)(2 3)(3 4)	(4 5)(2 3)(1 2)(2 3)(3 4)	

Commutation classes

Definition

We say that two reduced expressions are commutation equivalent if we can obtain one from the other by only commuting disjoint adjacent 2-cycles. (That is, don't apply any braid relations.)

This is an equivalence relation that partitions the set of reduced expressions for a given permutation. A single equivalence class is called a commutation class.

That is, a commutation class of a permutation σ is a subset of all reduced expressions for σ that can be obtained from one another by commuting disjoint cycles (never apply a braid relation).

Let's return to our previous example.

Example

The set of 11 reduced expressions for (1 3 5 4) forms two commutation classes:

(1 2)(2 3)(1 2)(4 5)(3 4)	(1 2)(2 3)(4 5)(1 2)(3 4)	(1 2)(4 5)(2 3)(1 2)(3 4)
(1 2)(2 3)(4 5)(3 4)(1 2)	(1 2)(4 5)(2 3)(3 4)(1 2)	(4 5)(1 2)(2 3)(3 4)(1 2)
(4 5)(1 2)(2 3)(1 2)(3 4)		

↕ (1 2)(2 3)(1 2) = (2 3)(1 2)(2 3)

(2 3)(1 2)(2 3)(4 5)(3 4)	(2 3)(1 2)(4 5)(2 3)(3 4)	(2 3)(4 5)(1 2)(2 3)(3 4)
(4 5)(2 3)(1 2)(2 3)(3 4)		

The longest element

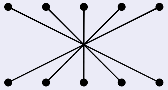
Recall that the length of a reduced expression is the number of adjacent 2-cycles appearing in the expression.

Definition

The longest element in S_n is the (unique) element having maximal length. The longest element is usually denoted by w_0.

Comments

1. w_0 has length $\dfrac{n(n-1)}{2}$.
2. The permutation diagram for w_0 is of the form ($n = 5$ here):



3. Every adjacent 2-cycle appears at least once in every reduced expression for w_0.
4. The number of reduced expressions for w_0 in S_n is known. But...

What we don't know is:

Open problem

How many commutation classes does the longest element in the symmetric group have?

That is, given the set of reduced expressions for w_0, how many equivalence classes does the commutation equivalence relation partition the set into?

Of course, for a given n, we could work really hard to figure out the answer (the bigger n is, the harder we'd have to work). But what we want is a general solution.

A (good) solution would either be a function of n or a recurrence relation.

Example

In S_3, the longest element is (1 3). In this case, there are two equivalence classes.

$$\boxed{(1\ 2)(2\ 3)(1\ 2)} \qquad \boxed{(2\ 3)(1\ 2)(2\ 3)}$$

Example

In S_4, the longest element is (1 4)(2 3). In this case, there are 8 equivalence classes.

(2 3)(1 2)(3 4)(2 3)(3 4)(1 2)	(2 3)(3 4)(1 2)(2 3)(3 4)(1 2)
(2 3)(3 4)(1 2)(2 3)(1 2)(3 4)	(2 3)(1 2)(3 4)(2 3)(1 2)(3 4)

(1 2)(3 4)(2 3)(3 4)(1 2)(2 3)	(3 4)(1 2)(2 3)(3 4)(1 2)(2 3)
(1 2)(3 4)(2 3)(1 2)(3 4)(2 3)	(3 4)(1 2)(2 3)(1 2)(3 4)(2 3)

(1 2)(2 3)(3 4)(1 2)(2 3)(1 2)	(1 2)(2 3)(1 2)(3 4)(2 3)(1 2)

(3 4)(2 3)(3 4)(1 2)(2 3)(3 4)	(3 4)(2 3)(1 2)(3 4)(2 3)(3 4)

(2 3)(1 2)(2 3)(3 4)(2 3)(1 2)

(2 3)(3 4)(2 3)(1 2)(2 3)(3 4)

(1 2)(2 3)(3 4)(2 3)(1 2)(2 3)

(3 4)(2 3)(1 2)(2 3)(3 4)(2 3)

- According to the On-Line Encyclopedia of Integer Sequences, the number of commutation classes of the longest element in $S_1, S_2, \ldots, S_{11}$ is 1, 1, 2, 8, 62, 908, 24698, 1232944, 112018190, 18410581880, 5449192389984, respectively.
- Many people have worked on this problem: R. Stanley (& some of his students), B. Tenner, A. Björner, D. Knuth, S. Elnitsky, R. Bedard, Bailly, Mosseri, Destainville, Widom, Kassel, Lascoux, Reutenauer, H. Denoncourt ("Heroin Hero"), me (but only a little), etc.
- This problem is related to primitive sorting networks (computer science), oriented matroids (math), pseudoline arrangements (math), rhombic tilings (math/physics), Schubert cells (math), and stability of quasicrystals (physics).
- If you want to know more, please ask.
- Lastly, please come talk to me if you come up with a solution for arbitrary n.