Discrete Mathematics lecture notes 11-2

November 22, 2013

30. A combinatorial description of the parity of a permutation

In the previous lecture we proved

Theorem 1. *For each $\sigma \in \Sigma_n$, the parity of the number of transpositions needed to express σ is well-defined.*

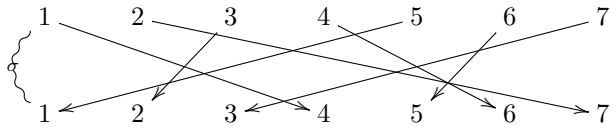
by proving the reduction

Proposition 2. *If $\mathrm{id} = \tau_1\tau_2\ldots\tau_n$ is an expression of the identity of Σ_m as a product of transpositions, then n is even.*

Here, we'll reprove Proposition 2 using a more combinatorial approach.

Definition 3. Fix $\sigma \in \Sigma_n$ and a pair (i, j) with $1 \leq i < j \leq n$. The (i, j) is an *inversion* for σ if $\sigma(i) > \sigma(j)$.

That is, an inversion is an ordered pair whose order is flipped by σ. It turns out to be easiest to visualize inversions using the modified row description of permutations. For example, if $\sigma = (1465)(273)$, then



which may look like a mess, except that all we're really interested in is the number of crossing.

Proposition 4. *For a fixed $\sigma \in \Sigma_n$, a pair (i, j) with $1 \leq i < j \leq n$ is an inversion for σ if and only if the lines originating at i and j cross. In particular, the number of inversions is the total number of intersections of lines in the row presentation of σ.*

For our example, it is easy to check that the inversions are

$$(1,3)\ (1,5)\ (1,7)\ (2,3)\ (2,5)\ (2,7)\ (2,6)\ (3,5)\ (4,5)\ (4,7)\ (4,6)\ (6,7)$$

for a total of 12.

There are two lemmata[1] that makes the notion of inversion useful to us:

Lemma 5. *If τ is a transposition, then the number of inversions of τ is odd.*

Lemma 6. *If τ is a transposition and σ is an arbitrary permutation, then $\tau \circ \sigma$ has an odd number of inversions more than σ.*

Proof of Proposition 2 given Lemmata 5 and 6. If we have an expression of the form $\mathrm{id} = \tau_1\tau_2\ldots\tau_{n-1}\tau_n$, then the number of inversions of id equals that of the composite of transpositions. As id has zero inversions, we conclude the number of inversions of the composite must also be zero, which happens to be an even number.

Consider: τ_n has an odd number of inversions by Lemma 5, so we can't have $n = 1$. $\tau_{n-1}\tau_n$ has an odd number of inversions more than an odd—that is, an eve—number of inversions by Lemma 6, so $n = 2$ is a possibility. $\tau_{n-2}(\tau_{n-1}\tau_n)$ has an odd number more than an even number—so an odd number—of inversions, so $n = 3$ is impossible. Etc. We conclude that if n is odd, the composite has an odd number of inversions, contrary to our assumption that the composite is the identity. Proposition 2 follows. □

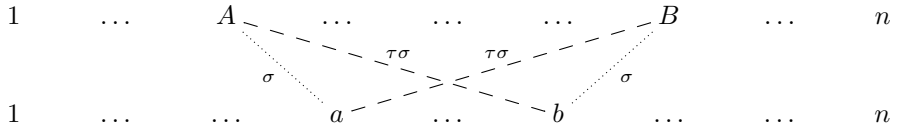
So all we have to do is prove Lemmata 5 and 6.

[1] Yay Greek pluralization! What other examples of this do you know?

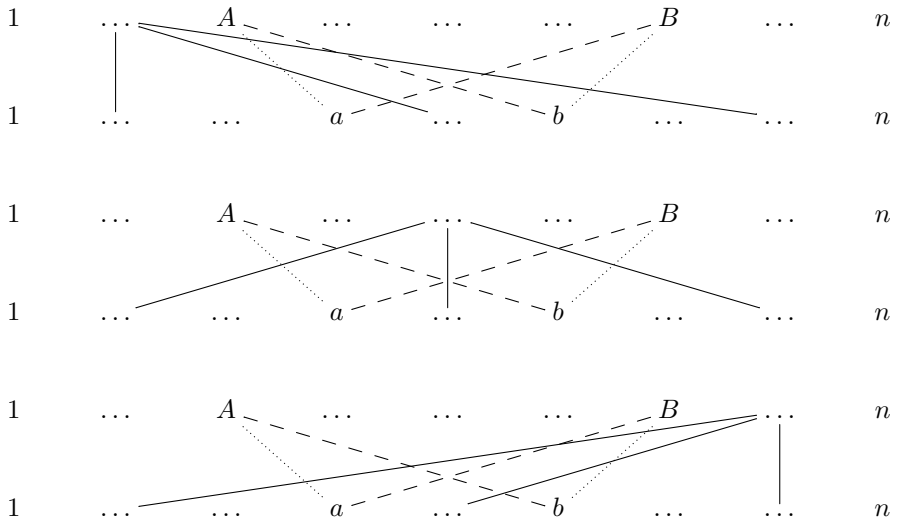
Proof of Lemma 5. Fix a transposition $\tau = (a, b)$ with $a < b$. Since τ only changes a and b, for any pair (i, j) with $1 \leq i < j \leq n$, the only way that (i, j) could be an inversion for τ is if either $i = a$ or $j = b$. The complete list of inversions with $i = a$ is $\{(a, a+1), (a, a+2), \ldots (a, b)\}$,[2] of which there are $b - a$. Similarly, the complete list of inversions with $j = b$ is $\{(a, b), (a+1, b), \ldots, (b-1, b)\}$, of which there are again $b - a$. Of course, we've double counted the inversion (a, b), so the total number of inversions is $2(b - a) - 1$, which is visibly odd. □

Proof of Lemma 6. Fix the permutation σ and $\tau = (a\ b)$. Set $A := \sigma^{-1}(a)$ and $B := \sigma^{-1}(b)$; without loss of generality assume that $A < B$.[3]

Let α denote the number of inversions for σ and β the number of inversions for $\tau\sigma$. By our description of the number of inversions as the number of intersections of lines in the modified row presentation of the permutation, the difference $\beta - \alpha$ will depend on how postcomposing with τ affects the tangle of lines. It turns out there's a very simple answer.



In this diagram, we're only recording the difference between σ and $\tau\sigma$: Because τ only acts by swapping a and b, only the two pairs of lines indicated are changed: The dotted line represents the action of σ and the dashed line the action of $\tau\sigma$. All other lines will be drawn in solid, as below, and are not changed by the passage from σ to $\tau\sigma$. In particular, the number of intersections of solid lines with other solid lines are not changed, and all we're really interested in for the difference $\beta - \alpha$ is how the number of intersections with solid lines with dotted lines compares to the number of intersections of solid lines with dashed lines.



This tidy mess is actually representing the nine possibilities of a solid line in the presentation of σ and $\tau\sigma$: The origin (=top) of the line can be less than A, between A and B, or greater than B; similarly for the terminus (=bottom). We're now interested in the number of intersections of each of these lines with the dotted versus dashed lines: You can check for yourself that the *difference* between these numbers is always even.

This seems to suggest that $\beta - \alpha$ is even, contrary to the conclusion of the Lemma. However, we're forgetting the dotted and dashed lines themselves. Visually there are no intersections between the dotted

[2] Verify this by drawing the row presentation of τ.

[3] If not, replace σ by $\tau\sigma$ and run the argument that way.

lines, and one intersection between dashed. Putting all this together, we conclude that $\beta - \alpha$ is odd, as desired. □

Definition 7. A permutation $\sigma \in \Sigma_n$ is *even* if σ can be written as a product of an even number of transpositions; otherwise σ is odd.

The point of the main Theorem for this week is that the notion of even/odd is well-defined, as is

Definition 8. Let $\operatorname{sgn} : \Sigma_n \to \{\pm 1\}$ be the function $\operatorname{sgn}(\sigma) = \begin{cases} +1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}$.

Proposition 9. *For all $\sigma_1, \sigma_2 \in \Sigma_n$, we have* $\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1) \cdot \operatorname{sgn}(\sigma_2)$.

Proof. Clear. □

This is a particular case of what is called a *group homomorphism*. This should be thought of as function between groups that preserves the multiplicative structure, or the "right" notion of function between groups. This also allows us to define a particular *subgroup* of Σ_n.

Definition 10. The *alternating group* of degree n is $A_n := \{\sigma \in \Sigma_n | \operatorname{sgn}(\sigma) = +1\}$.

What we've actually been showing is that A_n is closed under multiplication and inversion, a condition that we will explore in more detail in the next week. For now, we'll just tease some more advance algebra courses by waving our hands and saying that A_n for $n \geq 5$ is in a well-defined sense indecomposable, and that this (surprisingly) closely related to the fact that there is no closed form description[4] of the roots of a polynomial of degree of five or greater.

Exercise. Take a course in Galois theory and flesh out this relationship.

[4]That is, while there is a quadratic formula—the roots of $ax^2 + bx + c$ are $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$—and more complicated formulas for the roots of degree 3 and 4 polynomials, there is no quintic or higher formula.