The Sign of a Permutation

Matt Baker

Let σ be a *permutation* of $\{1,2,\ldots,n\}$, i.e., a one-to-one and onto function from $\{1,2,\ldots,n\}$ to itself. We will define what it means for σ to be *even* or *odd*, and then discuss how the parity (or *sign*, as it is called) behaves when we multiply two permutations. Finally, we will prove a useful formula for the sign of a permutation in terms of its cycle decomposition.

Two-line representation

One way of writing down a permutation is through its *two-line representation*

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

For example, the permutation α of $\{1,2,3,4,5,6\}$ which takes 1 to 3, 2 to 1, 3 to 4, 4 to 2, 5 to 6, and 6 to 5 has the two-line representation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 6 & 5 \end{pmatrix}$.

Graphic representation

We can visualize the permutation σ as a (bipartite) graph G_σ by writing the numbers $1,2,\ldots,n$ in two rows and joining i (in the top row) to $\sigma(i)$ (in the bottom row) with an edge for all i. For example, the graph corresponding to the permutation α above is:

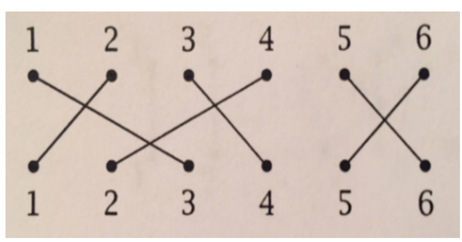

Figure 1: The graph G_α

Inverting and multiplying permutations

Given a permutation σ, its *inverse* σ^{-1} is the permutation sending $\sigma(i)$ to i for all $i = 1,\ldots,n$. For example, the inverse of the permutation α and β above is $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$. In terms of the graphic representation, inverting a permutation corresponds to interchanging the top and bottom rows of the corresponding graph.

Given permutations σ and τ of $\{1, 2, \ldots, n\}$, their *product* $\sigma\tau$ is the function $i \mapsto \sigma(\tau(i))$, i.e., we compose the two permutations as functions. Note that in general $\sigma\tau \neq \tau\sigma$; for example, if α is as above and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 4 & 2 \end{pmatrix}$, then $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ and $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 1 & 2 & 4 \end{pmatrix}$.

In terms of graphic representations, to compute $\sigma\tau$ we concatenate the diagrams corresponding to each, with τ placed above σ. For example, the following picture represents $\beta\alpha$ in our running example:

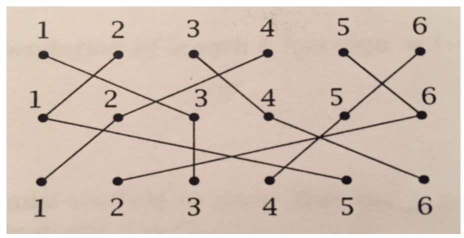

Figure 2: Graphical representation of $\beta\alpha$

Cycle decomposition

Another way of writing down a permutation is through its *cycle decomposition.* A permutation σ is called a k*-cycle* if there exist distinct elements $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$ such that

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1,$$

and $\sigma(i) = i$ for all other i. We denote such a cycle by $\sigma = (i_1\ i_2\ \cdots\ i_k)$. A 2-cycle is also called a *transposition.* Note that every element of a cycle can be considered as the starting point, so for example $(1234) = (2341)$.

The basic fact about permutations and cycles is the following:

Lemma: Any permutation can be written as a product of disjoint cycles. This representation is unique, apart from the order of the factors and the starting points of the cycles.

We will not give a formal proof of this result (though it's not difficult), but will instead describe the algorithm underlying its proof and give some examples.

Algorithm: (Decompose a permutation into a product of disjoint cycles)

WHILE there exists $i \in \{1, \ldots, n\}$ not yet assigned to a cycle:

- Choose any such i;
- Let ℓ be the smallest positive integer such that $\sigma^\ell(i) = i$;
- Construct the cycle $(i\ \sigma(i)\ \cdots\ \sigma^{\ell-1}(i))$.

RETURN the product of all cycles constructed.

Example: The cycle decomposition of α is (1342)(56). Indeed, if we start with $i = 1$ then following the above algorithm we have $\ell = 4$ and we construct the cycle (1342). We next choose the unused element $i = 5$ and construct the cycle (56), and we're done.

Similarly, the cycle decomposition of β is (15462)(3). It is customary to omit fixed elements in cycle notation, so we could also write β as simply (15462).

Note that (1234) and (2341), for example, determine the same cycle, and that (12)(34) and (34)(12) represent the same permutation. We can make the cycle decomposition *unique* by requiring that each cycle begins with its smallest element, and that the cycles are ordered with increasing smallest elements.

Inversions and signature

A pair (i, j) with $i, j \in \{1, 2, \ldots, n\}$ is called an *inversion* of σ if $i < j$ but $\sigma(i) > \sigma(j)$. The *inversion number* $\mathrm{inv}(\sigma)$ is the total number of inversions of σ. The permutation σ is called *even* (resp. *odd*) if $\mathrm{inv}(\sigma)$ is even. The *sign* of σ is defined as $\mathrm{sign}(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$. So $\mathrm{sign}(\sigma) = 1$ if σ is even and $\mathrm{sign}(\sigma) = -1$ if σ is odd.

It is easy to see that a pair (i, j) is an inversion of σ if and only if the edges $i\sigma(i)$ and $j\sigma(j)$ cross in the graphic representation of σ. Thus the inversion number $\mathrm{inv}(\sigma)$ equals the number of crossings in G_σ. This observation implies that $\mathrm{inv}(\sigma) = \mathrm{inv}(\sigma^{-1})$, and hence $\mathrm{sign}(\sigma) = \mathrm{sign}(\sigma^{-1})$.

The sign is multiplicative

We have the following fundamental formula:

$$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma) \cdot \mathrm{sign}(\tau). \tag{1}$$

To see this, note that (i, j) is an inversion in $\sigma\tau$ if and only if the paths starting at i and j cross in the top half of the composite graph but not the bottom, or in the bottom half but not the top. If they cross in both, as with 5 and 6 in Figure 2 above, then the crossings cancel out (in the figure, (5,6) is not an inversion for $\beta\alpha$). Thus $\mathrm{inv}(\sigma\tau) \equiv \mathrm{inv}(\sigma) + \mathrm{inv}(\tau) \pmod 2$, which is equivalent to (1).

The sign and cycle decompositions

Suppose $\sigma = \sigma_1\sigma_2\cdots\sigma_t$ is the cycle decomposition of a permutation σ. Applying (1) repeatedly, we see that

$$\mathrm{sign}(\sigma) = \mathrm{sign}(\sigma_1)\cdots\mathrm{sign}(\sigma_t). \tag{2}$$

So in order to compute the sign of an arbitrary permutation, it suffices to compute the sign of a cycle.

We first consider the sign of a transposition $\tau = (i, j)$. We claim that τ is odd. To see this, note that an edge kk with $k < i$ or $k > j$ contributes no crossing, while each edge kk with $i < k < j$ contribute two crossings (see Figure 3 below). There is only one additional edge, namely ij, which contributes one crossing. Thus the total number of crossings is odd, as claimed.

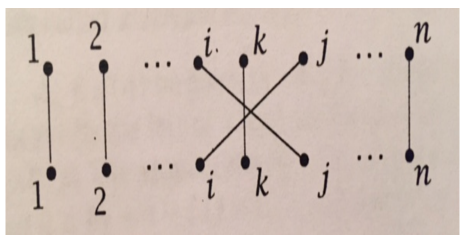

Figure 3: Crossings in a transposition

Now let $(i_1 i_2 \cdots i_\ell)$ be a cycle of length $\ell \geq 3$. One checks easily that

$$(i_1 i_2 \cdots i_\ell) = (i_1 i_2)\cdots(i_{\ell-2} i_{\ell-1})(i_{\ell-1} i_\ell)$$

and therefore the sign of an ℓ-cycle (for all $\ell \geq 1$) is $(-1)^{\ell-1}$. In other words, odd cycles are even and even cycles are odd.

By formula (2), we conclude that if the cycle decomposition of σ is $\sigma_1\sigma_2\cdots\sigma_t$ and σ_i has length ℓ_i, then

$$\mathrm{sign}(\sigma_1\sigma_2\cdots\sigma_t) = (-1)^{\sum_{i=1}^{t}(\ell_i - 1)}. \tag{3}$$

Naturality

In addition to being a useful computational tool, formula (1) shows that the sign of a permutation is *intrinsic*, in the following sense. Suppose we replace 1 by $\tau(1)$, 2 by $\tau(2)$, etc. in both rows of the two-line representation of σ, where τ is some permutation. Then σ is transformed into the *conjugate permutation* $\sigma' = \tau^{-1}\sigma\tau$. By (1), we have

$$\mathrm{sign}(\sigma') = \mathrm{sign}(\tau^{-1})\mathrm{sign}(\sigma)\mathrm{sign}(\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau)^2 = \mathrm{sign}(\sigma),$$

so that σ and σ' have the same sign.

This implies, in particular, that while the *number of inversions* of σ depends on our choice of an ordering of the set $\{1, 2, \ldots, n\}$, the *sign* of σ does not.

For an application to number theory, suppose p is an odd prime and g is a primitive root modulo p, and let a be an integer not divisible by p, so that $a \equiv g^k$ for some integer k. Let σ be the permutation of $\{1, 2, \ldots, p-1\}$ induced by multiplication by a modulo p and let σ' be the permutation of $\{0, 1, \ldots, p-2\}$ induced by addition of k modulo $p-1$. Then $\sigma' = \tau^{-1}\sigma\tau$, where $\tau : \{0, 1, \ldots, p-2\} \to \{1, 2, \ldots, p-1\}$ is defined by $\tau(j) \equiv g^j \pmod{p}$. By (1), the sign of σ is equal to the sign of σ'. (This is an important point in Zolotarev's proof of the Law of Quadratic Reciprocity.)

Acknowledgments

I have drawn from two main sources for this handout: Martin Aigner's "A Course in Enumeration" and Peter J. Cameron's "Combinatorics". The three figures above are all from Aigner's book.