M7210 Lecture 3 August 24, 2012

Permutations

Let X be a set with n elements, which we label $1, 2, \ldots, n$.

Definition. A *permutation* of X is a bijective function $\sigma : X \to X$.

Table notation. We may describe a permutation σ by a table of the following form:

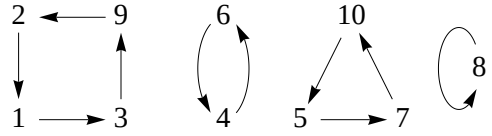
$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Because σ is bijective, each element of X occurs exactly once on the second line.

Example 1. The table below shows a permutation of $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ with $\sigma(1) = 3$, $\sigma(2) = 1$, etc.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 9 & 6 & 7 & 4 & 10 & 8 & 2 & 5 \end{pmatrix}$$

Pictures. One may visualize a permutation σ by means of a directed graph, where the vertices are the elements of X and there is an arrow from x to y if $y = \sigma(x)$. There is one arrow for every column in table notation. The permutation in Example 1 can be pictured as follows:



Since σ is bijective, each element of X has one arrow coming from it and one arrow going to it. This implies, according to the following lemma, that if we start at any element and follow the arrows, we eventually return to that element without ever passing through any other element more than once. In general, the graph may have many connected components as in the picture, or just one.

Lemma 1. *Let σ be a permutation of X. If k is the smallest (strictly) positive integer such that $\sigma^k(x) = x$, then the elements of $\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\}$ are all distinct.*

Proof. Suppose $\sigma^\ell(x) = \sigma^m(x)$, where $0 \le \ell \le m < k$. Apply $\sigma^{-\ell}$ to both sides to get $x = \sigma^{m-\ell}(x)$. But $0 \le m - \ell < k$, so by the the assumption on k, $m - \ell = 0$. /////

Cycles. A permutation is called a k-cycle (or a cycle of length k) if it fixes all but k elements—which we may name $a_0, \ldots a_{k-1}$—and acts on those according to:

$$\sigma(a_0) = a_1\ , \quad \sigma(a_1) = a_2\ , \quad \cdots \quad (a_{k-2}) = a_{k-1}\ , \quad \sigma(a_{k-1}) = a_0.$$

Such a cycle is denoted by listing the elements it moves between parentheses in such a manner that the image of each element is listed immediately after it:

$$\sigma = (a_0\ a_2\ \cdots\ a_{k-1}).$$

We may start with any element in the cycle:

$$(a_0\ a_1\ \cdots\ a_{k-2}\ a_{k-1}) = (a_1\ a_2\ \cdots\ a_{k-1}\ a_0) = \cdots = (a_{k-1}\ a_0\ \cdots\ a_{k-2}).$$

A cycle of length 1 is the identity permutation. A cycle of length 2 is called a *transposition*. Two cycles are said to be disjoint if they have no elements in common.

When using cycle notation to denote permutations, we use square braces to indicate the argument of a function:

$$(2\ 4\ 6\ 9)[4] = 6 \qquad (2\ 4\ 6\ 9)[9] = 2 \qquad (2\ 4\ 6\ 9)[3] = 3.$$

To evaluate a product of cycles, we work from the right.

$$\begin{aligned}(1\,3\,5)(2\,3\,7)(1\,5\,7)[2] &= (1\,3\,5)(2\,3\,7)\Big[(1\,5\,7)[2]\Big] \\ &= (1\,3\,5)(2\,3\,7)[2] \\ &= (1\,3\,5)\Big[(2\,3\,7)[2]\Big] \\ &= (1\,3\,5)[3] = 5\end{aligned}$$

Direct computation shows that if γ and δ are disjoint cycles, then $\gamma\delta = \delta\gamma$.

Cycle decomposition. Suppose σ is a permutation of X. Choose any element x of X. After it, write $\sigma(x)$. After that, write $\sigma(\sigma(x)) = \sigma^2(x)$, and continue until $\sigma^k(x) = x$. (The last element written is $\sigma^{k-1}(x)$.) Write the result as a k-cycle:

$$\Big(x\ \sigma(x)\ \sigma^2(x)\ \cdots\ \sigma^{k-1}(x)\Big).$$

After this, choose an element of X that is not in $\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\}$, and repeat. Write the corresponding cycle after the one previously written. Continue choosing previously unused elements and writing out the cycles they traverse until every element of X has been named. The end result will appear in following form:

$$\Big(x_1\,\sigma(x_1)\cdots\sigma^{k_1-1}(x_1)\Big)\Big(x_2\,\sigma(x_2)\cdots\sigma^{k_2-1}(x_2)\Big)\cdots\Big(x_m\,\sigma(x_m)\cdots\sigma^{k_m-1}(x_m)\Big), \qquad (*)$$

where

1) x_{i+1} is an element of X that does not occur among the $\sigma^j(x_s)$ with $s \le i$;
2) each element of X appears exactly once among the $\sigma^j(x_i)$;
3) $\sigma^{k_i}(x_i) = x_i$;

4) each k_i is ≥ 1—when $k_j = 1$, then the cycle containing x_j is (x_j).

Example 1 (continued). In cycle notation, the permutation in the table looks like this:

$$(1\,3\,9\,2)(4\,6)(5\,7\,10)(8). \qquad /////$$

Lemma 2. *Every permutation can be written as a product of disjoint cycles, and the cycles that appear in any such expression of a given permutation are the same, up to order.*

Proof. The existence is a direct consequence of the algorithm for cycle decomposition which we just described. For uniqueness, let $\gamma_1, \ldots, \gamma_s$ be disjoint cycles, and let $\delta_1, \ldots, \delta_t$ be disjoint cycles. Suppose

$$\gamma_1 \cdots \gamma_s = \delta_1 \cdots \delta_t.$$

Select any element of γ_1. It must appear in one of the δ_is, and that in which it does must equal γ_1. Multiply left and right by γ_1^{-1}, thus removing it from both sides. By induction, the remaining cycles are the same on both sides. /////

Lemma 3. *A cycle of length k can be written as a product of $k-1$ transpositions:*

$$(a_0\, a_2\, \cdots\, a_{k-1}) = (a_0\, a_{k-1})(a_0\, a_{k-2}) \cdots (a_0\, a_3)(a_0\, a_2)(a_0\, a_1).$$

Note that the transpositions are not disjoint. We see from Lemma 3 that every permutation is a product of transpositions. There is no uniqueness. For example $(a\,b\,c) = (a\,c)(a\,b) = (b\,a)(b\,c) = (c\,b)(c\,a)$. We will show, however, that *if σ is any permutation, then the parity (even or odd) of the number of factors in any decomposition of σ into transpositions is the same.*

Lemma 4. *Suppose $k, \ell \geq 0$, and $a, c_1, \cdots, c_k, b, d_1, \cdots, d_\ell$ are distinct elements of X. Then:*

$$(a\,b)(a\,c_1 \cdots c_k\, b\, d_1 \cdots d_\ell) = (b\, d_1 \cdots d_\ell)(a\, c_1 \cdots c_k),$$

$$(a\,b)(b\, d_1 \cdots d_\ell)(a\, c_1 \cdots c_k) = (a\, c_1 \cdots c_k\, b\, d_1 \cdots d_\ell).$$

In case $k = 0$, Lemma 4 asserts that $(a\,b)(a\,b\,d_1 \cdots d_\ell) = (a)(b\,d_1 \cdots d_\ell)$. If $k = \ell = 0$, we are saying $(a\,b)(a\,b) = (b)(a)$. The proof of Lemma 4 is by direct computation.

Definition. Suppose σ is written as a product of m disjoint cycles of length $k_1, \ldots, k_m$. Let $N(\sigma) := (k_1 - 1) + (k_2 - 1) + \cdots + (k_m - 1)$. Let $\operatorname{sgn}\sigma = (-1)^{N(\sigma)}$.

If τ is a transposition, $N(\tau) = 1$ and $\operatorname{sgn}\tau = -1$. Let us apply N to the permutations in Lemma 4:

$$N\big((a\, c_1 \cdots c_k\, b\, d_1 \cdots d_\ell)\big) = k + \ell + 1,$$

$$N\big((b\, d_1 \cdots d_\ell)(a\, c_1 \cdots c_k)\big) = k + \ell.$$

Lemma 5. Suppose τ is a transposition and σ is any permutation. Then

$$\operatorname{sgn}(\tau\sigma) = (-1)\operatorname{sgn}\sigma.$$

Proof. Suppose $\tau = (a\,b)$. Write σ as a product of disjoint cycles, allowing factors of the form (a) or (b) if a or b does not occur in any other cycles, and write the cycles containing a and b first. If a and b both occur in the initial cycle of σ, then by the first line of Lemma 4, $N(\sigma)$ is odd iff $N(\tau\sigma)$ is even. If a and b occur in different cycles in σ, then by the second line of Lemma 4, $N(\sigma)$ is odd iff $N(\tau\sigma)$ is even. /////

Proposition. For any permutations α and β of X,

$$\operatorname{sgn}(\alpha\beta) = (\operatorname{sgn}\alpha)(\operatorname{sgn}\beta).$$

Proof. Let m be the minimum number of transpositions required to write α. We use induction on m, the case $m = 1$ having been proved in Lemma 5. Note that if $\alpha = \tau_1\tau_2\cdots\tau_m$, then $\tau_2\cdots\tau_m$ cannot be written with fewer than $m-1$ transpositions. Thus

$$\begin{aligned} \operatorname{sgn}(\alpha\beta) &= (-1)\operatorname{sgn}(\tau_2\cdots\tau_m\beta) && \text{by Lemma 5} \\ &= (-1)\operatorname{sgn}(\tau_2\cdots\tau_m)(\operatorname{sgn}\beta) && \text{by induction} \\ &= (\operatorname{sgn}\alpha)(\operatorname{sgn}\beta) && \text{by Lemma 5.} \end{aligned}$$

Homework

1) Suppose X is a set with n elements (n a positive integer) and $f : X \to X$ is any function (not necessarily bijective). Let $X_{[k]} := \{\, f^k(x) \mid x \in X \,\}$, and let $f_{[k]}$ be the restriction of f to $X_{[k]}$. Show that there is $K < n$ such that $f_{[k]}$ is a permutation of $X_{[k]}$ for all $k \geq K$.
2) If the positive integers $(k_1, k_2, \ldots, k_m)$ in $(*)$ are listed in decreasing order, the sequence is called the *type* of the permutation. The type is simply a list of the cycle lengths. How many different types are there if X has 5 elements? 6? 7?
3) Suppose $\sigma = (a_0\, a_1\, \cdots\, a_{99})$. Write the following in cycle notation: σ^{-1}, σ^2, σ^3, σ^4, σ^5, σ^6, σ^7.
4) Suppose σ is a permutation of a set with n elements. Let $t(\sigma)$ be the number of cycles in σ, including 1-cycles. (E.g., if σ is the permutation in Example 1, $t(\sigma) = 4$.) Show that $\operatorname{sgn}\sigma = (-1)^{n-t(\sigma)}$.
5) Suppose that p is a non-constant function from the set of permutations of a finite set X to $\{-1, 1\}$ with the property that

   $$p(\alpha\beta) = p(\alpha)\,p(\beta), \text{ for all permutations } \alpha \text{ and } \beta.$$

   Show that $p = \operatorname{sgn}$.
6) Prove the statement in italics just before Lemma 4.