Math 51H Lecture Supplement
Permutations

A permutation on n elements is an ordered n-tuple $(i_1, \ldots, i_n)$ which is a re-ordering of the first n positive integers $1, \ldots, n$; that is the set $\mathcal{P}_n$ of all such permutations is

$$\mathcal{P}_n = \{(i_1, \ldots, i_n) : \{i_1, \ldots, i_n\} = \{1, \ldots, n\}\}.$$

Notice that there are exactly $n!$ such permutations.

Let $1 \le k < \ell \le n$, and define $\tau_{k,\ell} : \mathbb{R}^n \to \mathbb{R}^n$ by

$$\tau_{k,\ell}(x_1, \ldots, x_n) = (x_1, \ldots, x_\ell, \ldots, x_k, \ldots, x_n)$$

(i.e. $\tau_{k,\ell}$ interchanges the elements at position k, ℓ). Such a transformation is called a transposition; notice that $\tau_{k,\ell}$ is its own inverse. Thus $\tau_{k,\ell} \circ \tau_{k,\ell} =$ identity transformation on $\mathbb{R}^n$:

$$\tau_{k,\ell} \circ \tau_{k,\ell}(x_1, \ldots, x_n) \equiv (x_1, \ldots, x_n)\ \forall\, (x_1, \ldots, x_n) \in \mathbb{R}^n.$$

We claim that any permutation can be achieved by applying a finite sequence of such transpositions. Indeed if $(i_1, \ldots, i_n)$ is any permutation then we can write this permutation in terms of a permutation of the first $n-1$ (instead of n) integers as follows:

$$(i_1, \ldots, i_n) = \begin{cases} (\overbrace{i_1, \ldots, i_{n-1}}^{\text{perm. of } 1, \ldots, n-1}, n) & \text{if } i_n = n \\ \tau_{k,n}(\underbrace{i_1, \ldots, \underset{k^{\text{th}}\text{slot}}{i_n}, \ldots, i_{n-1}}_{\text{perm. of } 1, \ldots, n-1}, n) & \text{if } i_n < n \text{ (i.e. } i_k = n \text{ for some } k < n), \end{cases}$$

and so by induction on n it follows that each permutation can indeed be achieved by a sequence of transpositions; that is, for any permutation $(i_1, \ldots, i_n)$ we can find a sequence $\tau^{(1)}, \ldots, \tau^{(q)}$ of transpositions such that

$$(i_1, \ldots, i_n) = \tau^{(1)} \circ \tau^{(2)} \circ \cdots \circ \tau^{(q)}(1, \ldots, n). \tag{1}$$

Correspondingly we can permute the n coordinates $x_1, \ldots, x_n$ of a point in $\mathbb{R}^n$ using the same sequence of transpositions:

$$(x_{i_1}, \ldots, x_{i_n}) = \tau^{(1)} \circ \tau^{(2)} \circ \cdots \circ \tau^{(q)}(x_1, x_2, \ldots, x_n). \tag{1$'$}$$

Note: We of course do not claim the representation (1) is unique, and it is not—indeed there are many different ways of writing a given permutation in terms of a sequence of transpositions. For example if $n = 3$ then the permutation $(3, 2, 1)$ can be written as $\tau_{1,3}(1, 2, 3)$ but also as $\tau_{2,3} \circ \tau_{1,2} \circ \tau_{2,3}(1, 2, 3)$.

An important quantity related to a permutation $(i_1, \ldots, i_n)$ is the integer $N(i_1, \ldots, i_n)$, which is defined as the *number of inversions* present in the sequence $i_1, \ldots, i_n$; that is

$$N(i_1, \ldots, i_n) = \text{ the number of pairs } k, \ell \in \{1, \ldots, n\} \text{ with } k < \ell \text{ and } i_k > i_\ell.$$

This allows us to define the "parity" (i.e. "evenness" or "oddness") of a permutation:

Definition: The permutation $(i_1, \ldots, i_n)$ is said to even or odd according as the integer $N(i_1, \ldots, i_n)$ is even or odd.

Notice that then

$$(-1)^{N(i_1,\ldots,i_n)} = \begin{cases} +1 & \text{if } (i_1, \ldots, i_n) \text{ is even} \\ -1 & \text{if } (i_1, \ldots, i_n) \text{ is odd.} \end{cases}$$

The quantity $(-1)^{N(i_1,\ldots,i_n)}$ is called the index of the permutation $(i_1, \ldots, i_n)$.

Lemma. *If $1 \le k < \ell \le n$ and if $(i_1, \ldots, i_n)$ is a permutation of $(1, \ldots, n)$, then the index $(-1)^{N(i_1,\ldots,i_\ell,\ldots,i_k,\ldots,i_n)}$ has the opposite sign to the original index $(-1)^{N(i_1,\ldots,i_n)}$:*

$$(-1)^{N(i_1,\ldots,i_\ell,\ldots,i_k,\ldots,i_n)} = -(-1)^{N(i_1,\ldots,i_n)}.$$

Remarks: Notice that $(i_1, \ldots, i_\ell, \ldots, i_k, \ldots, i_n)$ can be written in terms of the transposition $\tau_{k,\ell}$ as $\tau_{k,\ell}(i_1, \ldots, i_n)$, so the above lemma says that *the parity of the permutation changes each time we apply a transposition*; notice in particular this means that the index $(-1)^{N(i_1,\ldots,i_n)}$ can be written alternatively as

$$(-1)^{N(i_1,\ldots,i_n)} = (-1)^q,$$

where q is the number of transpositions appearing in (1) above.

Proof of the Lemma: If $\ell = k+1$, then $N(i_1, \ldots, i_\ell, \ldots, i_k, \ldots, i_n) = N(i_1, \ldots, i_{k+1}, i_k, \ldots, i_n)$, and evidently (by counting inversions) we have

$$N(i_1, \ldots, i_{k+1}, i_k, \ldots, i_n) = \begin{cases} N(i_1, \ldots, i_k, i_{k+1}, \ldots, i_n) + 1 & \text{if } i_{k+1} > i_k \\ N(i_1, \ldots, i_k, i_{k+1}, \ldots, i_n) - 1 & \text{if } i_{k+1} < i_k, \end{cases}$$

and in either case the index differs by a factor -1 from the original index.

In the case when $\ell \ge k+2$ we can get the permutation $i_1, \ldots, i_\ell, \ldots, i_k, \ldots, i_n$ from $i_1, \ldots, i_n$ by first applying a sequence of $\ell - k$ transpositions of adjacent elements to move i_k to the right of i_ℓ, and then making a sequence of $\ell - k - 1$ transpositions of adjacent elements to move i_ℓ back to the k^{th} position. In all that is $2(\ell - k) - 1$ transpositions of adjacent elements, each changing the index by a factor of -1, so the total change in the index is $(-1)^{2(\ell-k)-1} = -1$, and the lemma is proved.

The inverse of the permutation $(i_1, \ldots, i_n)$ is the permutation $(j_1, \ldots, j_n)$ which "undoes" $(i_1, \ldots, i_n)$; that is, for each $k = 1, \ldots, n$, j_k is defined to be the unique element in $\{1, \ldots, n\}$ such that $i_{j_k} = k$, since $i_1, \ldots, i_n$ is just a rearrangement of $1, \ldots, n$, this means that $j_1, \ldots, j_k$ is also a rearrangement of $1, \ldots, n$ and is of course uniquely determined by $(i_1, \ldots, i_n)$. Also $i_{j_k} = k$ means in particular (replacing k by i_k) that $i_{j_{i_k}} = i_k$, which of course means that $j_{i_k} = k$; that is, $(i_1, \ldots, i_n)$ is the inverse of $(j_1, \ldots, j_n)$ (not surprising: it just says that the inverse of the inverse is the original permutation); notice in particular this guarantees that every permutation is an inverse (namely it is the inverse of its own inverse!), so the mapping $\varphi : \mathcal{P}_n \to \mathcal{P}_n$ which takes each given permutation $(i_1, \ldots, i_n)$ to its inverse $(j_1, \ldots, j_n)$ is onto and hence also 1:1

(any mapping of a finite set of elements onto itself is automatically 1:1 just by an elementary counting argument).

In terms of a sequence of transpositions $\tau^{(1)}, \ldots, \tau^{(q)}$ which give $(i_1, \ldots, i_n)$ as in (1), we have

$$(x_{i_1}, \ldots, x_{i_n}) = \tau^{(1)} \circ \tau^{(2)} \circ \cdots \circ \tau^{(q)}(x_1, x_2, \ldots, x_n)$$

and hence applying $\tau^{(q)} \circ \tau^{(q-1)} \circ \cdots \circ \tau^{(1)}$ to each side we get

$$\tau^{(q)} \circ \tau^{(q-1)} \circ \cdots \circ \tau^{(1)}(x_{i_1}, \ldots, x_{i_n}) = (x_1, x_2, \ldots, x_n)$$

and applying this with $(x_1, \ldots, x_n) = (j_1, \ldots, j_n)$, and using $j_{i_k} = k$, we see that

$$\tau^{(q)} \circ \tau^{(q-1)} \circ \cdots \circ \tau^{(1)}(1, \ldots, n) = (j_1, j_2, \ldots, j_n)$$

That is, the inverse $(j_1, \ldots, j_n)$ is given by

$$(j_1, \ldots, j_n) = \tau^{(q)} \circ \tau^{(q-1)} \circ \cdots \circ \tau^{(1)}(1, 2, \ldots, n)$$

(i.e. the same transpositions written in reverse order). In particular the index of the permutation $(i_1, \ldots, i_n)$ is the same as the index of the inverse $(j_1, \ldots, j_n)$, as both are equal to $(-1)^q$.