Transposition Distance of Permutations

Milind Hegde & Sabareesh Ramachandran

Theorem. Let $\hat{P} \in S_n$ and $P \in M_n(\mathbb{R})$ be the permutation matrix of $\hat{P}$. The minimum number of transpositions required to bring $\hat{P}$ to identity is $\text{rank}(I_n - P)$.

For example, if $\hat{P} \in S_2$ is the transposition $(1\ 2)$, then $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Clearly one transposition has to be applied to $\hat{P}$ to make it the identity, which must be the minimum. 1 is also the rank of $I_n - P = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$.

The elements in $\{1, \ldots, n\}$ fixed by $P$ correspond to the zero rows of $I_n - P$. The remaining rows will contain exactly one 1 and one $-1$ each. The same will apply to the columns of the matrix.

$I_n - P$ can be viewed as the incidence matrix of a directed graph $G$, where a column containing only zeroes is regarded as a 1-cycle. The rows of the incidence matrix correspond to the vertices of the graph. If $a_{ij} = 1$, the edge $e_j$ has its head at vertex $v_i$. If $a_{ij} = -1$, the edge $e_j$ has its tail at vertex $v_i$.

Since each column of the matrix sums to zero, every vertex of $G$ has indegree equal to outdegree, i.e. $G$ decomposes into cycles (by a simple theorem of graph theory). Since each row contains exactly one each of 1 and $-1$, these cycles are disjoint.

Lemma. The number of cycles (including 1-cycles of isolated vertices) of $G$ is equal to the nullity of the incidence matrix $M$ of $G$.

Proof. We will show that each cycle gives exactly one zero row through row transformations.

If a row contains only zeroes, it is a 1-cycle which clearly gives exactly one zero row to the matrix, and also contributes a single cycle to the graph. Hence we can consider only rows which are not zero rows.

Assume vertices $v_1, \ldots, v_k$ make up a cycle $C$ in $G$. Then their corresponding rows contain (in total) $k$ 1s and $k$ $-1$s. Since the columns correspond to the edges of $G$, each column contains exactly one pair of 1 and $-1$. Hence $k$ columns contain all the non-zero entries of the $k$ rows corresponding to $C$.

Now it is clear that summing the $k$ rows gives the zero row. Hence from the rows corresponding to $C$, we can get at least one zero row by row transformations.

If it were possible to get more than one zero row, that would imply that some subset of the $k$ rows (and hence $k$ vertices) can combine to form the zero row. WLOG, let this subset correspond to $v_1, \ldots, v_\ell$ with $\ell < k$. As these $\ell$ vertices form an incomplete part of a cycle, they form a path with one extra edge at each endpoint, and hence have $\ell - 1 + 2 = \ell + 1$ edges incident on them.

Thus the non-zero entries of the $\ell$ rows are spread over $\ell + 1$ columns, with no row or column containing only zeroes. This implies that one column contains a 1 and no $-1$, while another column contains $-1$ and no 1. Thus for a combination of the $\ell$ rows to give zero, the coefficients
of the two rows must be zero to make the columns zero. Then by induction we get that for the combination to be zero, all the coefficients must be zero. (Essentially the incidence matrix of a path with no cycles is of full rank.)

So every cycle contributes exactly 1 zero row through row transformations, meaning the number of possible zero rows = nullity($M$) is the number of cycles.

We write $(k \ell)$ to denote the permutation (as well as permutation matrix) that switches $k$ and $\ell$. 

WLOG say that the permutation $P$ takes 1 to $k$, $k \neq 1$. Then, $I_n - (1 \ k)P$ has first row zero. So it remains to be shown that

$$\text{rank}(I_n - P) = 1 + \text{rank}(I_n - (1 \ k)P)$$

in order to complete the proof by induction (on rank of $I_n - P$), where the base case of $P = I_n$ is trivially true.

**Proof.**

*Case 1: $P$ has $1 \to k$ and $k \to 1$.*

In this case, $I_n - (1 \ k)P$ will have both row 1 and row $k$ as zero, while the remaining rows are the same as in $I_n - P$. 

However, note that if 1 goes to $k$ and $k$ goes to 1, then the graph $G$ will contain the 2-cycle of $v_1$ and $v_k$. Then $I_n - (1 \ k)P$ having row 1 and row $k$ as zero corresponds to this 2-cycle being broken up into two isolated vertices, i.e. the number of cycles increases by 1 (as the rest of the graph is unchanged).

Hence by the lemma and the rank-nullity theorem, the nullity of $I_n - (1 \ k)P$ increases by 1, i.e.

$$\text{rank}(I_n - (1 \ k)P) = \text{rank}(I_n - P) - 1$$

*Case 2: $P$ has $1 \to k$ but not $k \to 1$.*

In this case, $I_n - (1 \ k)P$ will have row 1 as zero, and row $k$ will have a 1 and $-1$. Since $(1 \ k)P$ is also a permutation, $I_n - (1 \ k)P$ will maintain the property that every column sums to zero. So one of 1 and $-1$ (not both) in the $k$th row of $P$ will be displaced to maintain this property. The four non-zero entries of row 1 and row $k$ (in $P$) will be present in exactly three columns, with one column (say $\ell$) containing a non-zero entry for each of the two rows. Hence row $k$ will have the entry in column $\ell$ displaced to the column of the other non-zero entry of row 1.

The remaining rows of $I_n - (1 \ k)P$ are the same as in $I_n - P$. 

In terms of the graph $G$, initially $v_1$ and $v_k$ are in the same cycle, as they share an edge through the common column. After the transposition, $v_1$ becomes an isolated vertex, and $v_k$ is part of a cycle smaller by 1. As the remaining cycles are untouched, the number of cycles of $G$ in total increases by 1, as required. 

In fact, this proof does not use any property of the identity permutation, and hence can be directly generalized to count the minimum number of transpositions required to transform a permutation $P$ to a permutation $P'$. 

2