Crux Challenge Problem

Chris Long

August 31, 1999

Problem: Let $t_1, \ldots, t_m$ be transpositions such that $t_1 \cdot \ldots \cdot t_m = 1$ and the t_i generate S_n. Prove that $m \geq 2n - 2$.

Solution: Let $T = \{t_1, ..., t_m\}$, and observe that

$$(a\ b)(a\ c) = (a\ c)(b\ c) = (b\ c)(a\ b).$$

A set of transpositions generates S_n if and only if the "derived graph" is connected. The "derived graph" on the vertices $v_1, \ldots, v_n$ is obtained by joining v_a and v_b with an edge if our set of transpositions contains $(a\ b)$. The necessity is obvious, since if a and b are disconnected the transposition $(a\ b)$ cannot be generated by any product of our transpositions. For sufficiency, observe that for distinct a, b, x_i,

$$(a\ x_1)(x_1\ x_2) \ldots (x_k\ b)(x_k\ x_{k-1}) \ldots (x_1\ a) = (a\ b).$$

Actually, this should be a "derived hypergraph"; connect transpositions $(a\ b)$ and $(c\ d)$ if and only if they have some element in common. But this is just the dual graph of the above graph, and so one is connected if and only if the other is.

Now observe that if the derived graph of T is connected and $t_i = (a\ b)$ and $t_{i+1} = (a\ c)$, then the dervied graph of T' formed by replacing t_i with $(a\ c)$ and t_{i+1} with $(b\ c)$ (or with $(b\ c)$ and $(a\ b)$, respectively) is also connected (in fact, this is an if and only if). Furthermore, the ordered product of the t_i will still be 1 by the above identities.

The particular form of the identities we need is

$$(1\ a)(a\ b) = (a\ b)(1\ b) = (1\ b)(1\ a).$$

The key step now is that it follows from this, together with the fact that we may swap two adjacent transpositions that commute, that we may assume that *every* t_i has the form $(1\ x)$ for some x (this process would terminate prematurely if and only if the derived graph was disconnected). Since every $x \neq 1$ must appear at least once (by connectedness), every $x \neq 1$ must appear at least twice (otherwise the product would not be 1). Hence $|T| \geq 2 \cdot (n-1) = 2n - 2$. $\square$