Crypto Homework 3

Noah Wong

December 24, 2018

Graded Homework 3
Noah Wong
Professor Kubik
Math 5347
October 3, 2018

1.) (20 points) Let $\sigma = (1\,3\,5\,2)(7\,6)$ and $\tau = (2\,4\,5\,7)(3\,6)$ be elements of S_7.

a.) Compute σ^2 and write the answer as a product of dijoint cycles.

$\sigma = ((1\,3\,5\,2)(7\,6)$, so $\sigma^2 = (1\,3\,5\,2)(7\,6)(1\,3\,5\,2)(7\,6)$.

$$\sigma^2 = (1\,5)(2\,3)$$

b.) Compute $\tau\sigma$ and write the answer as a product of disjoint cycles.

$\tau = (2\,4\,5\,7)(3\,6)$ and $\sigma = (1\,3\,5\,2)(7\,6)$, so $\tau\sigma = (2\,4\,5\,7)(3\,6)(1\,3\,5\,2)(7\,6)$.

$$\tau\sigma = (1\,6\,2)(3\,7)(4\,5)$$

2.) (10 points) Write all the cycles of length three that live in S_4.

There are 8 cycles of length three, because in order to have a cycle of length 3 in S_4, one element must be sent to itself. Then there are 2 ways to arrange the remaining 3 elements into a cycle. So there every element sent to itself there are two ways to construct a cycle so $2 * 4 = 8$ cycles possible. They are as follows,

$$(2\,3\,4),\ \ (2\,4\,3),\ \ (1\,3\,4),\ \ (1\,4\,3),$$
$$(1\,2\,4),\ \ (1\,4\,2),\ \ (1\,2\,3),\ \ (1\,3\,2).$$

3.) (30 points) Label the corners of your Rubik's cube with the with numbers one through eight in the manner discussed in class.

a.) For each generating move of the Rubik's cube, write how the corners are moved using cyclic notation from S_8.

$$R = (2\,3\,8\,7)$$
$$L = (1\,6\,5\,4)$$
$$U = (1\,4\,3\,2)$$
$$D = (5\,6\,7\,8)$$
$$B = (3\,4\,5\,8)$$
$$F = (1\,2\,7\,6)$$

b.) Compute D^2, DR, URU, and $RDFD^2$.

We first break each move down into its permutation, taking the basic moves permutations from problem 3a.). Then we use permutation composition to find the final result.

$$D^2 = (5\,6\,7\,8)(5\,6\,7\,8) = (5\,7)(6\,8)$$

$$DR = (5\,6\,7\,8)(2\,3\,8\,7) = (2\,3\,5\,6\,7)$$

$$\begin{aligned} URU =& (1\,4\,3\,2)(2\,3\,8\,7)(1\,4\,3\,2) \\ URU =& (1\,4\,3\,2)(1\,4\,8\,7\,2) \\ URU =& (1\,3\,2\,4\,8\,7) \end{aligned}$$

$$\begin{aligned} RDFD^2 =& (2\,3\,8\,7)(5\,6\,7\,8)(1\,2\,7\,6)(5\,6\,7\,8)(5\,6\,7\,8) \\ RDFD^2 =& (2\,3\,8\,7)(5\,6\,7\,8)(1\,2\,7\,6)(5\,7)(6\,8) \\ RDFD^2 =& (2\,3\,8\,7)(5\,6\,7\,8)(1\,2\,7\,5\,6\,8) \\ RDFD^2 =& (2\,3\,8\,7)(1\,2\,8)(5\,7\,6) \\ RDFD^2 =& (1\,3\,8)(2\,7\,6\,5) \end{aligned}$$

c.) What moves would you use to interchange the front left upper corner with the down right back corner? Which other corner cubes are not in their original position when you do this?

The moves starting from left and going right are: $L- > B- > D- > D- > U- > U$. However when we write the moves as a product of permutations we start on the right and go left. This give us

$$
\begin{aligned}
U^2D^2BL &= (1\,4\,3\,2)(1\,4\,3\,2)(5\,6\,7\,8)(5\,6\,7\,8)(3\,4\,5\,8)(1\,6\,5\,4),\\
U^2D^2BL &= (1\,4\,3\,2)(1\,4\,3\,2)(5\,6\,7\,8)(5\,6\,7\,8)(1\,6\,8\,3\,4),\\
U^2D^2BL &= (1\,4\,3\,2)(1\,4\,3\,2)(5\,6\,7\,8)(1\,7\,8\,3\,4)(5\,6),\\
U^2D^2BL &= (1\,4\,3\,2)(1\,4\,3\,2)(1\,8\,3\,4)(5\,7),\\
U^2D^2BL &= (1\,4\,3\,2)(1\,8\,2)(5\,7),\\
U^2D^2BL &= (1\,8)(2\,4\,3)(5\,7).
\end{aligned}
$$

We can see that corners 2, 3, 4, 5 and 7 have all changed spots as well. Only 6 remains in its original position. Although 6 does change orientation so it's not truly in its original position. This is one of the problems with using permutations to represent cubies.