Core Algebra: Lecture 2, Solving Rubik's Cube Cont'd[1]

Recall from last time:
We want to show that for $M_1 = \{\sigma_{1j_1}\sigma_{2j_2}\dots\sigma_{nj_n} : \forall\, i,\ j_i \geq i \text{ and } \sigma_{ij_i} \in T\}$, $M_1 = G$.
$M_1 \subset G$ by construction and M_1 contains all the generators of G so if we show that M_1 is a group, then $M_1 = G$. Since M_1 is finite, it suffices to show it is closed under multiplication.

Claim 2.1. *(From last time) $M_k \cdot M_k \subset M_k$ (so M_k is a subgroup).*

Proof. (See handout.) Using backward induction.
$M_n = \{I\}$ so the claim is true for M_n.
Suppose $M_5 \cdot M_5 \subset M_5$. Subclaim: $\sigma_{8j_8}M_4 \subset M_4$. (Using 4, 5 and 8 instead of k, $k+1$ and any $l > k$).
Any element $\sigma \in \sigma_{8j_8}M_4$ is contained in $\sigma_{8j_8}(\sigma_{4j_4}M_5)$ for some σ_{4j_4}. But $\sigma_{8j_8}\sigma_{4j_4}$ is a product of elements in T so was also fed into T and by a claim from last time that means it can be expressed as a monotone product in $\sigma_{4j_4}M_5$. Using that $M_5 \cdot M_5 \subset M_5$, we get:
$\forall\, \sigma \in \sigma_{8j_8}M_4,\ \sigma \in (\sigma_{4j_4}M_5)M_5 \subset \sigma_{4j_4}M_5 \subset M_4$.
Now, $\forall\ \sigma \in M_4M_4$, σ is of the form $(\sigma_{4j_4}\sigma_{5j_5}\dots\sigma_{nj_n})(\sigma_{4j_4'}\sigma_{5j_5'}\dots\sigma_{nj_n'})$. From the above comments, $\sigma_{nj_n}(\sigma_{4j_4'}\sigma_{5j_5'}\dots\sigma_{nj_n'})$ can be expressed as a monotone product σ' in M_4. Then $\sigma_{(n-1)j_{n-1}}\sigma'$ can be expressed as a monotone product in M_4 and so on until we get that σ is a monotone product in M_4. So, $M_4M_4 \subset M_4$ and by induction $M_1M_1 \subset M_1$. $\square$

Answers to the questions from the beginning of the first lecture:

1. Since $M_1 = G$, from the definition of M_1 it follows that:
   $|G| =$ The product of the sizes of the columns of T.

2. To determine whether $\sigma \in S_n$ is in G, we obtain the table T using the described algorithm and then try to feed σ in T. If the result of that is writing in an empty cell of T, that means σ is not the product of elements in G and hence does not belong to G.

3. While creating T, we can keep track of the expression of each element in the table as a product of the generators of G. Then, for any $\sigma \in G$, we feed σ in T and get an expression $\sigma_{1j_1}^{-1}\dots\sigma_{kj_k}^{-1}\sigma = I$ which in turn gives is an expression for σ in terms of the generators of G.

4. To produce a random element of G with uniform distribution, we choose randomly one element from each column and multiply them.

Example

Understand $G = \langle \sigma_1 = 2\ 3\ 1\ 4, \sigma_2 = 2\ 1\ 4\ 3 \rangle \subset S_4$.

- Feed σ_1 … to σ_{12}.
- Feed $\sigma_{12}^2 = 3\ 1\ 2\ 4$ to σ_{13}.
- $\sigma_{12}^3 = I$ so the next nontrivial element or product of elements to feed is σ_2.
- Feed $\sigma_2 = 2\ 1\ 4\ 3$ … feed $\sigma_{12}^{-1}\sigma_2 = 1\ 3\ 4\ 2$ to σ_{23}.

[1]Notes from Professor Bar-Natan's Fall 2010 Algebra I class. All the mistakes are mine, please let me know if you find any! (ivahal@math.toronto.edu)

And so on, eventually we get $|G| = 4 \cdot 3 \cdot 1 \cdot 1 = 12 < 24 = |S_4|$.

(1,1) I			
(1,2) 1 $\sigma_{12} = \sigma_1 = 2\ 3\ 1\ 4$	(2,2) I		
(1,3) 2 $\sigma_{13} = \sigma_{12}^2 = 3\ 1\ 2\ 4$	(2,3) 3 $\sigma_{23} = \sigma_{12}^{-1}\sigma_2 = 1\ 3\ 4\ 2$	(3,3) I	
(1,4) 5 $\sigma_{23}\sigma_{13} = 4\ 1\ 3\ 2$	(2,4) 4 $\sigma_{13}^{-1}\sigma_{23}\sigma_{12} = 1\ 4\ 2\ 3$	(3,4) –	(4,4) I

The red numbers in the table indicate the order in which the cells were filled.

Question 1: $\sigma = 4\ 1\ 2\ 3\ \in\ G$?
If we try to feed σ, we see that it would go in cell $(1, 4)$ which is already occupied by 4 1 3 2 so we feed $(4\ 1\ 3\ 2)^{-1} 4\ 1\ 2\ 3$ which can be entered in the $(3, 4)$ cell which is empty. Hence, σ is not in G.

Question 2 What is the expression of $\sigma = 2\ 4\ 3\ 1\ \in\ G$ in terms of the generators?
We feed σ in T. It would have to go in cell $(1, 2)$ which is already filled so we feed $\sigma_{12}^{-1}\sigma = 1\ 4\ 2\ 3$ which would go in the already filled cell $(2, 4)$. We feed $\sigma_{24}^{-1}\sigma_{12}\sigma = I$. So, $\sigma = \sigma_{12}\sigma_{24}$ which in turn can be expressed in terms of the generators.

How good is the algorithm?
It works great in answering the first, second and fourth question but for the third, giving a solution to the cube, the words we get might be of exponential length. One way to make it more efficient is: when feeding σ to cell (i, j) which is already filled with a longer word σ_{ij}, we can put σ in place of σ_{ij} and feed $\sigma_{ij}^{-1}\sigma$.