Stephen Hutchins

CCS Math 103 200: Selected Topics from Discrete Math

Notes: Rubik's Cube Group Theory

Today's lecture is going to deal with **groups** as a topic in mathematics, and how Rubik's Cube permutations are related to groups. **SPOILER ALERT:** The set of all Rubik's Cube sequences form a group under the operation concatination (joining strings of moves together). But first, let us start by defining a group:

Definition. A **Group** $(G, \star)$ is a set G with a defined binary operation$\star$ that satisfies the following properties:

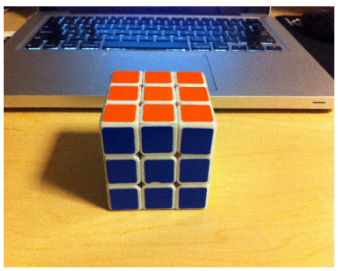
- **Closure:** i.e. for all $a, b \in G$, $(a \star b) \in G$
- **Associativity:** i.e. $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$
- **Existence of an Idenity:** i.e. there exists some element $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$
- **Existence of Inverses:** i.e. for all $a \in G$, there exists some element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$

And for those who don't know:

Definition. A **binary operation** $*$ on a set S is a function $f : S \times S \to S$: i.e. for all $a, b \in S$ there exists a unique $c \in S$ such that $a * b = c$.

Now that we have these definitions sorted out, I will start making steps to prove that Rubik's cubes do infact make groups. To do that though, let me first start by defining some notation to represent Rubik's cube sequences on paper.

A 90 degree clockwise rotation a face will expressed with a capital letter from the following set $\mathbb{M} = \{F, B_a, L, R, T, B_o\}$. F is rotating the front-most layer, B_a for the back-most layer, L for the left-most layer, R for the right-most layer, T for the top-most layer, and finally B_o for the bottom-most layer. Also, keep in mind that all of the layers are defined by looking at a cube from the perspective pictured below.



In addition, when I say "clockwise," I always mean clockwise relative to the face that is being rotated: i.e. which way would be clockwise if you were looking at the face in question directly. Finally, we add an exponent to the end of a letter top make it a 90 turn *counter*-clockwise (e.g. R^{-1}).

Now that we have all of that notation resolved, we can start talking about bigger things. First of which is: how do we define the set of all sequences on a Rubik's Cube?

Definition. The set of all rubik's cube sequences $\mathbb{P}_R$ is the set of all possible concatinations of elements from $\mathbb{M}$ with equivalence classes set up between sequences that, when applied to separate cubes, yield the same permutation.

Claim. $\mathbb{P}_R$ forms a group under the binary operation concatination.

To prove this claim, we will go through all of the group axioms one by one.

Proof. Let $\mathbb{P}_R$ be defined to have the operation concatination $*$.

1. **Closure:** $(\mathbb{P}_R, *)$ satisfies closure because a sequence of moves added to another sequence moves is still in the same set. In fact, the entire set $\mathbb{P}_R$ is defined from the generating set $\mathbb{M}$.

2. **Associativity:** Concatination is associative by definition: $a*(b*c) = (a*b)*c = abc$ for all $a, b, c \in \mathbb{P}_R$.

3. **Idenity:** There does exist an idenity element in $\mathbb{P}_R$: the empty sequence, i.e. the sequence in which no layers are rotated. We will call this element 0

4. **Inverses:** This is where the notation I defined earlier comes in handy. For all generating moves $m \in \mathbb{M}$, there exists some m^{-1} such that $m * m^{-1} = m^{-1} * m = 0$. That is, any clockwise rotation can be undone with the corresponding counter-clockwise rotation.

   Extending this idea to larger sequences, let $p = m_1 m_2 ... m_n$. Then $p^{-1} = m_n^{-1} ... m_2^{-1} m_1^{-1}$ since this results in $p * p^{-1} = p^{-1} * p = 0$.

□

Now since there exists a bijective relation between elements of $(\mathbb{P}_R, *)$ and Rubik's cube permutations, and Rubik's cubes have a finite number of permutations, $(\mathbb{P}_R, *)$ must form not just a group but also a finite group.