Group Theory Applied To Twisty Puzzles

Spencer T. Parkin

March 11, 2017

This paper explores the application of group theory to the problem of solving twisty puzzles, such as the Rubik's Cube. While many expositions on this subject have been given, this one aims to present the material in as straight-forward and concise a manner as to make it accessible to any undergraduate of mathematics having taken a course in modern algebra. Many accessible references will be given as we make our way through the paper.

1 The Problem Statement

We begin by formulating the twisty puzzle problem in terms of group theory. To do that, let us first discuss the way in which a permutation group models a given twisty puzzle. Simply put, after labeling the faces of such a puzzle with natural numbers in the solved state, we may conceive of the permutation (bijective map) that takes all of those labels to any given scrambled state of the puzzle. For puzzles that allow, not just rotation, but also reflection, such as the virtual puzzle shown in figure **??**, we may consider labeling the edges or vertices to accomplish the same task.

The set of all such permutations of the puzzle then forms a group under the operation of function composition. How do we know this? Because the group is generated by the set of permutations that form the basis for the puzzle. In the case of Rubik's Cube, there are six generators, one for each face of the cube.

Having now modeled a twisty puzzle in terms of a permutation group, we're ready to state the problem of solving such a puzzle in terms of group theory. Given any permutation of the group (given any state of the puzzle),

find a factorization of that element in terms of the generators of the group. Of course, it's really the inverse of this factorization that we're after, but that is easily found by inverting all generators found the factorization, and then writing them down in reverse order. Thus, we need only focus our efforts on finding the sequence of generator permutations that take us from the solved state of the puzzle to the given scrambled state.

2 The Factorization Problem

Let's first consider the brute-force attack on the problem. Given any permutation $g \in G$, we go search for its factorization by systematically enumerating all elements of $G = \langle S \rangle$. One way to do this is to perform a breadth-first search of the Cayley graph of G. (See **??**.) In such a graph, the vertices are group elements, and directed edges connect a group element $a \in G$ to $b \in G$ if there can be found $s \in S$ such that $as = b$ or $as^{-1} = b$. As we traverse the graph, our path from the identity element to our current vertex gives us our factorization of the element at that location. Since we're guarenteed to reach all elements of G, we'll certainly find g, at which point we'll have our solution! In practice, of course, we would also need to build the graph as we traverse it, since the only information we have to start with is S. Being breadth-first, our solution should be as short as possible.

For small groups, this approach is feasible, but what about the Rubik's Cube? According to **??**, the number of possible permutations of the Rubik's Cube is upwards of 4 *quintillion*! Clearly, we need a better way. Enter the subgroup chain!

Suppose we have a nested sequence of subgroups $\{G_k\}_{k=1}^{n}$ such that

$$G = G_1 > G_2 > \cdots > G_n = \{e\}.$$

Suppose further, for each subgroup, we have $G_k = \langle S_k \rangle$ with T_k, a set of elements taken from G such that $|T_k| = |G_{k-1}|/|G_k|$, and

$$G_{k-1} = \bigcup_{t \in T_k} G_k t.$$

Here, T_k is what's called a right transversal of the cosets of G_k in G_{k-1}. Each element in T_k is called a coset representative. Any element of a coset may serve as a representative.

Gathering all this information is a matter of concern, but let's first talk about using it to solve our problem. Given any $g \in G$, our procedure is as follows. Let $f = e$ be the identity element. Find k such that $g \in G_{k-1}$, but $g \notin G_k$. If there is no such k, then $g \in G_n \implies g = e$, and we're done. Otherwise, we make the observation that there exists $t \in T_k$ such that $G_k t = G_k g$, and therefore, $gt^{-1} \in G_k$. Assign gt^{-1} to g, and ft^{-1} to f, and repeat at the point where we find k. When we're done, f^{-1} is the desired factorization, and f itself is the solution to the puzzle!

Of course, for this to work, we need there to be a known way of writing every element in T_k and S_k in terms of the generators in S_{k-1}. This will naturally fall out of our process of generating the subgroup chain.

To that end, let's consider now the construction of a subgroup chain for our permutation group. In this case, a natural choice of nested subgroups arrises as those being characterized by the set of all permutations that stabilize a given point in our domain Ω. This is the set upon which each of our permutations $g \in G$ is defined, and we say that G is a subgroup of $\mathrm{Sym}(\Omega)$, the symmetric group of order $|\Omega|!$. (See **??**.) Refering back to our Rubik's Cube, we may think of each point in Ω as a sticker on our cube.

Now, if the stabilizer subgroups were normal, transversals would always be the representatives of a cyclic factor group. But alas, they're not. Nevertheless, we have the orbit-stabilizer theorem! But first, let's introduce a few definitions and notation.

For any $\omega \in \Omega$, and any $g \in G$, we will let ω^g denote the image of ω under the permutation g.[1] The set of all possible images of ω over G will be denoted by ω^G and given by

$$\omega^G = \{\omega^g | g \in G\}.$$

The set of all permutation in G stabilizing a given $\omega \in \Omega$ will be denoted by G^ω, and given by

$$G^\omega = \{g \in G | \omega^g = \omega\}.$$

That said, we now establish a bijection between T and ω^G. Map $t \in T$ to $\alpha \in \omega^G$, where $\omega^t = \alpha$. Let $a, b \in T$ such that $\omega^a = \omega^b$. Then $\omega^{ab^{-1}} = \omega \implies ab^{-1} \in G^\omega \implies G^\omega a = G^\omega b \implies a = b$, since T contains one and only one representative for each right coset of G^ω in G. It follows now that since $|T| = |\omega^G|$, we have

$$|G| = |\omega^G||G^\omega|.$$

[1] We avoid the notation $g(\omega)$ so as not to confuse it with the convenient cycle-notation.

This is the orbit-stabilizer theorem, but what we're really interested in is the proof; for it tells us that the problem of generating the transversal T of G^ω in G is related to the problem of generating the orbits of ω in G. For every new orbit we find, we also find a new coset representative in T.

At this point we can return to the idea of traversing the Cayley graph of G, but instead of needing to traverse until we find g, we just need to run until, for every $\alpha \in \omega^G$, we've encountered an element t in G taking ω to α.

Having a transversal T of G^ω in G, the last piece of the puzzle is a way to generate generators for G^ω in terms of S and T, and this is where Schreier's lemma **??** comes into play. His lemma states

$$G^\omega = \langle \{ st\overline{st}^{-1} | s \in S \text{ and } t \in T \} \rangle,$$

where here, for any $g \in G$, we're using the notation $\bar{g}$ to mean the element in T such that $G^\omega \bar{g} = G^\omega g$. These are called Schreier generators, and the union of all generators in a stabilizer chain form what's called a strong generating set for G. It's strong, because that union, when restricted to any subgroup in the chain, still generates that subgroup.

We now give a proof of Streier's lemma taken from **??**. Do that here...

Now that we have Streier's lemma, and the orbit-stabilizer theorem, we have everything we need to recursively construct the stabilizer chain! Generate T_k from S_k and our characterization of G_{k+1}, then S_{k+1} from S_k and T_k.

3 A Drawback To The Solution

Like the brute-force attack, the method thus described, unfortunately, has its own serious drawback. As we descend the chain, the size of the factorizations (words) of the elements in T_k and S_k in terms of the original generators S of G become more than exponentially larger with linear growth in k. An idea of Minkowitz **??**, however, can be used to mitgate this problem.