The Group Structure of the Rubik's Cube

Richard Wong
Rutgers University

December 2, 2016

1 Introduction

The Rubik's Cube is a familiar toy that has embedded itself into popular culture since its invention in 1974 by Ernő Rubik. It is especially popular among mathematicians, for good reason. In this paper, we will investigate some of the interesting mathematical structure underlying the Rubik's Cube, which was documented by David Joyner in his book, *Adventures in Group Theory* [Joy].

Let us consider a standard Rubik's cube, unmarked, $3 \times 3 \times 3$ Rubik's Cube. Furthermore, we will imagine that we fix the center facets of the cube, so that we do not need to consider the three-dimensional rotational symmetry of the Rubik's Cube. We can then scramble and unscramble the cube in the traditional sense through a sequence of cube moves.

Definition 1.1 A **cube move** is the rotation of a particular face in the clockwise direction by 90°.

We will refer to these cube moves using the Singmaster notation. We write the set of cube moves as $\{F, B, U, D, R, L\}$, where the cube move F rotates the "front" face, B rotates the opposing "back" face, U rotates the "top" face, D rotates the opposing "bottom" face, R rotates the "right" face, and L rotates the opposing "left" face.

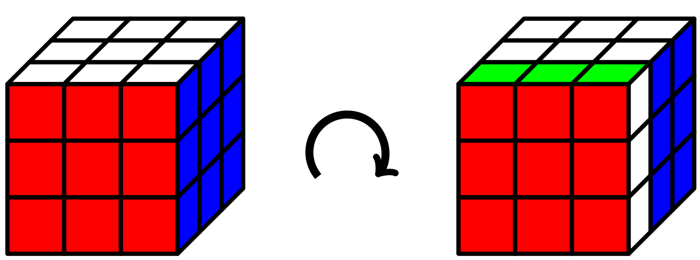

Figure 1: Applying the cube move F.

Definition 1.2 A **legal position** of a standard Rubik's Cube is any permutation of the Rubik's Cube that can be reached from the solved Rubik's Cube through a sequence of cube moves.

It follows from the definition that the set of legal positions is generated by the six cube moves. Furthermore, it turns out that the set of legal positions of a standard Rubik's Cube forms a group. This is because we can identify a legal position with a sequence of cube moves. However, since different sequences of cube moves may result in the same legal position, we see that there will be many group relations.

Theorem 1.3 *The set of legal positions of a Rubik's Cube forms a group G, with the operation on legal positions being the concatenation of corresponding sequences of cube moves. We will call this group G the* ***Rubik's Cube Group****.*

With this identification and the given group operation, it is simple to verify that the axioms of closure and associativity are satisfied. The identity element is the solved Rubik's Cube, which corresponds to the empty sequence of cube moves.

Furthermore, we expect that any legal position has an inverse, because there are algorithms for solving a Rubik's Cube. This is true, since each cube move has an inverse. For every cube move C, we have that $C^4 = Id$, hence $C^3 = C^{-1}$. Therefore, every legal position has an inverse as well, since the cube moves generate the legal positions. If we have a sequence of cube moves $C_1C_2\cdots C_{n-1}C_n$ corresponding to a legal position, the inverse of that legal position corresponds to the sequence of cube moves $C_n^{-1}C_{n-1}^{-1}\cdots C_2^{-1}C_1^{-1}$.

We also note that G is not abelian, since $FR \neq RF$.

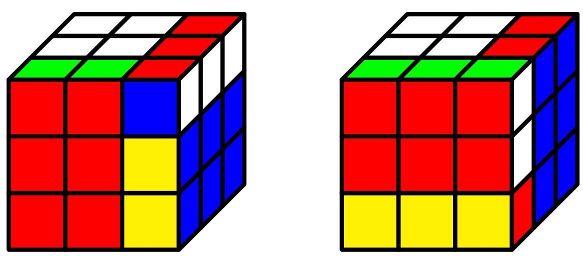

Figure 2: FR, left, versus RF, right.

2 The order of G

It is natural to ask how large the group G is, or equivalently, how many legal positions there are. One would hope that G is finite, and we will see that it is. In fact, its order can be calculated by purely combinatorial means.

To see that G is finite, we note that we can view G as a subgroup of the permutations of the facets of the Rubik's Cube. The Rubik's Cube has 6 faces, with 9 facets each, for a total of 54 facets. Of these facets, because we have fixed the 6 center facets, there are 48 facets that can be permuted. Therefore, we can embed G as a subgroup of S_{48} by mapping the cube moves $\{F, B, U, D, R, L\}$ according to how they permute the facets.

However, it is clear that not all permutations of the facets are possible due to the physical constraints of the cube. For example, we cannot swap a facet on an edge block with a facet on a corner block. We also do not allow ourselves to "swap the stickers" on the cube, so if a facet on a single block is permuted, the other facets on the same block must also be permuted accordingly.

Furthermore, not all permutations that respect this physical constraint are possible. If the Rubik's Cube is disassembled and then reassembled, we will see that the probability of obtaining a solvable Rubik's Cube (in other words, an element of G) is only 1 in 12. For example, if we take a solved Rubik's Cube, and we flip the orientation of a single edge block, it becomes impossible to solve the cube through the cube moves.

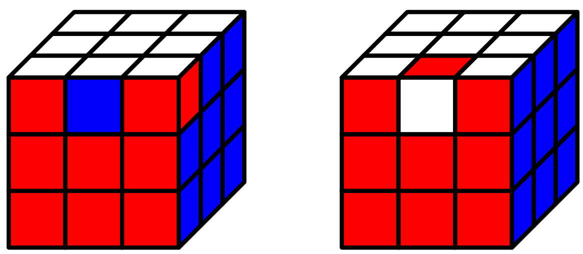

Figure 3: Two Rubik's Cubes that are not legal positions.

Before we calculate the order of the group G, let us simply consider how large it is:

$$|G| = 8!12! * 2^{10} * 3^7 = 2^{27} * 3^{14} * 5^3 * 7^2 * 11 = 43252003274489856000$$

There are over 43 quintillion legal positions of the cube. The original packaging of the Rubik's Cube stated that "there were more than three billion possible states the cube could attain". While they were technically correct, Douglas Hofstadter compared this claim as being analagous to "McDonald's proudly announcing that they've sold more than 120 hamburgers" [Pa].

To calculate the order of G, we observe that if we disassemble and reassemble the Rubik's Cube, there are 8 corner blocks, and 12 edge blocks, and we can permute them independently of each other. We can place each corner block in 3 different orientations, and we can place each edge block in 2 different orientations. So there are at most $(8!) * (12!) * 3^8 * 2^{12}$ elements in G. But this is an overestimate by a factor of twelve.

To observe this, we first note that the permutation of blocks after applying a cube move has even parity. Since every legal position is generated by the cube moves, every legal position corresponds to an even permutation of the blocks. Therefore, only half of the full set of assemblies are valid. Physically, this shows that we cannot interchange a single pair of blocks. However, we can swap two pairs of edge blocks, two pairs of corner blocks, a pair of corner blocks and a pair of edge blocks, or cycle three blocks of the same kind. Note that these interchanges are exactly those used in the PLL algorithm for solving the Rubik's Cube.

There are also restrictions on the orientations of the edge blocks and on the orientation of the corner blocks. For each edge block position, we assign a vector parallel or anti-parallel to the edge that borders no other blocks.

This collection of vectors determines the orientations of the edge blocks in the following way. We assign this collection of vectors to the edge blocks in the solved Rubik's cube. Then, given a sequence of cube moves corresponding to a legal position, we can track how the vectors are permuted by the sequence of cube moves.

Definition 2.1 A given edge block has **negative orientation** if its corresponding vector is anti-parallel to the vector assigned to the position occupied by the given edge block. Otherwise, it has **positive orientation**.

Given a collection of vectors, for at least one cube move, the orientation of edge blocks of the corresponding face is non-trivially permuted by the cube move. In fact, given an orientation on the cube, each cube move flips the orientation of exactly zero, two, or four edge blocks of the corresponding face. As a corollary, it is impossible to flip the orientation of a single block. Therefore, of the assemblies of even parity, only half will have the proper edge block orientation.

In an analogous way, we can assign a collection of vectors to the corner blocks, which determines the orientation of the corner blocks. It turns out that a cube move twists the orientation of corner blocks so that only a third of the remaining assemblies are valid [Che], [Da]. Therefore, out of the initial set of assemblies of the Rubik's Cube, only one in twelve are actually obtainable from the cube moves. Therefore, we have determined the order of G by counting: $|G| = 8!12! * 2^{10} * 3^7$.

3 The Structure of G

It turns out that G has a special kind of group structure. It is an example of a semi-direct product of groups, which is a generalization of the direct product of groups.

Definition 3.1 We say a group H is an (inner) semi-direct product if it has subgroups N, K such that the following conditions hold:

1. $N \trianglelefteq H$
2. $H = NK = \{nk | n \in N, k \in K\}$
3. $N \cap K = \{Id_H\}$

Then we write $H = N \rtimes K$. Clearly, direct products are examples of inner semi-direct products. However, unlike the direct product, the subgroups N, K do not uniquely specify $N \rtimes K$.

Example 3.2 Both $\mathbb{Z}_6$ and S_3 can be written as $\mathbb{Z}_3 \rtimes Z_2$.

Since the direct product is an example of an inner semi-direct product, and since $\gcd(2,3) = 1$, we have that

$$\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 = \mathbb{Z}_3 \rtimes Z_2$$

Now let us consider the following subgroups of S_3, $N = \langle (123) \rangle \cong \mathbb{Z}_3$ and $K = \langle (12) \rangle \cong \mathbb{Z}_2$. Since $[S_3 : N] = 2$, we have that $N \trianglelefteq S_3$. Furthermore, it is easy to see that $S_3 = NK$ and $N \cap K = \{Id_{S_3}\}$. Therefore,

$$S_3 = N \rtimes K = \mathbb{Z}_3 \rtimes Z_2$$

However, if we are given a map $\Phi : K \to \mathrm{Aut}N$ sending $k \mapsto \Phi_k$, such that $(nk)(n'k') = (n\Phi_k(n'))(kk')$, then N, K, and Φ define H up to isomorphism. For our purposes, the map $\Phi : K \to \mathrm{Aut}N$ is a conjugation action: $\Phi_k(n) = knk^{-1}$.

To see that G has the semi-product structure, let us consider the following subgroups of G. Let G_O be the subgroup of legal positions that fix the blocks but permute their orientations. And let G_P be the subgroup of legal positions that fix the orientations but permute the blocks. It is useful to construct these subgroups explicitly in terms of sequences of cube moves, and we can do so in the following way.

Definition 3.3 The **normal closure** of a subset A of a group H, $N_{Cl}(A)$, is the intersection of all normal subgroups in H that contain A.

$$N_{Cl}(A) = \bigcap_{A \subseteq N, N \trianglelefteq H} N$$

It follows that $N_{Cl}(A)$ is a normal subgroup of H.

We can write G_O as the normal closure of the following two sequences of cube moves, where the former flips the orientation of adjacent edge blocks, and the latter twists the orientation of opposite corner blocks.

$$\{BR^{-1}D^2RB^{-1}U^2BR^{-1}D^2RB^{-1}U^2, RUDB^2U^2B^{-1}UBUB^2D^{-1}R^{-1}U^{-1}\}$$

We can also write G_P as the subgroup generated by the following sequences of cube moves, where the last sequence of cube moves cyclically permutes three edge blocks.

$$\{U^2, D^2, F, B, R^2, L^2, R^2U^{-1}FB^{-1}R^2F^{-1}BU^{-1}R^2\}$$

It is clear that $G_O \cap G_P = Id_G$, since the only legal position resulting from a sequence of cube moves that fixes both the blocks and their orientations is the solved cube.

Furthermore, G_O is normal in G. This follows from the construction of G_O as the normal closure of a subset. However, we can also see that G_O is normal in G in the following way. If we have an element $n \in G_O$, and an element $g \in G$, then the sequence of cube moves gng^{-1} is in G_O. This is because g will permute the blocks, n will fix the blocks, and g^{-1} will undo the permutation of g, and so gng^{-1} fixes the blocks.

To see that $G = G_O G_P$, which would therefore show that $G = G_O \rtimes G_P$, we look at the sizes and structures of the two subgroups.

We claim that $G_O = \mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}$, where $\mathbb{Z}_m^n$ is the direct product of n copies of $\mathbb{Z}_m$. This follows from our earlier investigation: We can twist each corner block independently in three ways, but because of the restriction on the orientation of corner blocks, the orientation of the last corner is determined by the other seven. Similarly, we can flip the edge blocks independently in two ways, but again, the orientation of the last is determined by the first eleven. And because the orientation of edges is independent of the orientation of corners, G_O has the above structure.

We claim that $G_P = (A_8 \times A_{12}) \rtimes \mathbb{Z}_2$. We note that the group of even permutations of only edge blocks (A_8) and of the group of even permutations of only corner blocks (A_{12}) are both normal in G_P. Therefore, their (inner) direct product, $A_8 \times A_{12}$, is also normal in G_P.

We note that the subgroup generated by a single permutation that swaps a pair of edge blocks and a pair of corner blocks is isomorphic to Z_2. It acts on $A_8 \times A_{12}$ by conjugation by the permutation.

The intersection of the subgroups of G_P is again equivalent to the solved cube. Furthermore, any permutation of blocks that fixes orientations can be generated by conjugating a permutation in $A_8 \times A_{12}$ by the permutation that generates $\mathbb{Z}_2$. Therefore , G_P has the above structure.

Examining the orders, $|G_O| = 3^7 * 2^{11}$, and $|G_P| = (\frac{8!}{2})(\frac{12!}{2}) * 2$, so the order of $G_O G_P$ is $8!12! * 2^{10} * 3^7 = |G|$. So we see that G does indeed have the semi-direct product structure:

$$G = (\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}) \rtimes ((A_8 \times A_{12}) \rtimes \mathbb{Z}_2)$$

4 Generalizations

In our analysis of the Rubik's Cube Group, we restricted our attention to a standard, unmarked, $3 \times 3 \times 3$ cube with fixed centers, and we looked only at the legal positions of the Rubik's Cube. However, we can generalize our observations in a variety of ways.

What if we considered a Rubik's Cube with markings, and without fixing the centers? You may have noticed that unlike a standard Rubik's Cube, a specially made Rubik's Cube with a picture or some other kind or marking is more difficult to solve because the orientations of the center facet must now be accounted for. A Rubik's Cube with markings would then have the group structure:

$$\mathbb{Z}_4^6 \times \big((\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}) \rtimes ((A_8 \times A_{12}) \rtimes \mathbb{Z}_2)\big)$$

What if, instead of considering the legal positions, we consider the possible positions obtained from disassembling and reassembling the cube, or in other words, permuting the blocks freely? We saw that the order of this set of positions was $12 * |G|$, and it turns out that this set of positions has a group structure as well, where the operation is the concatenation of the permutations of the blocks. This group also has a special structure: namely, it is the direct product

$$\mathbb{Z}_4^6 \times (\mathbb{Z}_3 \wr S_8) \times (Z_2 \wr S_{12})$$

Where $A \wr H$ is the unrestricted wreath product of A and H, which is a special construction of a semi-direct product. In particular, the wreath product $\mathbb{Z}_m \wr S_n$ is known as the generalized symmetric group $S(m,n)$. In this case, the structure of $\mathbb{Z}_m \wr S_n = \mathbb{Z}_m^n \rtimes S_n$, and we have the action $\Phi : S_n \to \text{Aut}\mathbb{Z}_m^n$ that sends $\sigma \mapsto \big((z_1, z_2, \ldots z_n) \mapsto (z_{\sigma(1)}, z_{\sigma(2)}, \ldots z_{\sigma(n)})\big)$ [Joy].

In the case of the group of the free permutation of the blocks, we can view $\mathbb{Z}_4^6$ as the permutations of the center facets, $\mathbb{Z}_3 \wr S_8$ as the permutations of the corner blocks, and $Z_2 \wr S_{12}$ as the permutations of the edge blocks, all three of which are independent of each other.

Other interesting generalizations to consider are the $n \times n \times n$ Rubik's Cubes, or other similar mechanical puzzles such as the Skewb, Magic Dodecahedron, and even 4-D puzzles such as the Magic 120-Cell, or the Magic Cube 4D (a $4 \times 4 \times 4 \times 4$ puzzle). Joyner's book [Joy] has given some partial results on the group structure of these puzzles. The underlying structure of 2D mechanical puzzles, also known as sliding puzzles, have been studied as well. An example is the well-known 15 puzzle, which has a groupoid structure [Jo].

These underlying structures provide interesting natural examples to investigate, and can lead to developing efficient algorithms for solving these puzzles. Furthermore, it seems possible to proceed in the reverse direction as well: given a group G, one might try to construct a puzzle or toy that has G as its natural underlying structure.

References

[Che] Chen, Janet : Group Theory and the Rubiks Cube. 2004.

[Da] Davis, Tom : Group Theory Via Rubik's Cube. 2006.

[Dav] Davies, J. W.; Morris, A. O., "The Schur Multiplier of the Generalized Symmetric Group", J. London Math. Soc (2), 8, (1974), pp. 615-620.

[Jo] Johnson, Wm. Woolsey; Story, William E. (1879), Notes on the "15" Puzzle, American Journal of Mathematics (The Johns Hopkins University Press) 2 (4): 397404.

[Joy] Joyner, David : Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys. Johns Hopkins University Press, 2008.

[Pa] Paulos, J.A. : Innumeracy: Mathematical Illiteracy and Its Consequences. Farrar, Straus and Giroux, 2011.