THE RUBIK'S GROUP

NATHAN MCANALLY

1. Introduction

In 1974, a toy was created that would confuse the world. This toy was a rather simple puzzle created by a Hungarian architect by the name of Erno Rubik. His puzzle was a simple 3x3 cube with six different colors. Each face could be twisted causing the colors to get mixed up around the cube. A few years later, this toy got its now household name: The Rubik's Cube.

The story of this toy coming to be an international icon is quite interesting. Since Hungary was behind the Iron Current in 1974, the Soviet Communist would not be very accepting of such a toy. In order for this toy to gain the international fame it received by 1980, it would need to escape this communist regime. Since Rubik originally invented this toy as a mathematical model for his students, the Rubik's Cube found its way out of the Iron Current through mathematicians who would take the cube to conferences. At such conferences, the cube began to gain popularity, allowing it to break free of the Communist regime, and become almost instantly an international household toy. Since the cube hit the world market in 1980, approximately 350 million Rubik's Cubes have been sold and about one in every seven people have owned and/or played with a Rubik's Cube. [3]

2. Preliminaries

While any scientific mind can easily see that there are many mathematical properties of the Rubik's Cube, these properties do not really become clear until seen under the light of abstract algebra, or more specifically group theory. These concepts not only give a mathematical understanding of the so called "magic cube," but they also help professional cube solvers to rapidly solve the cube (even blindfolded). While many of these individuals may not have a complete understanding of the group theory at work behind their actions, it is certainly the driving motivation for all techniques regarding the cube. To come to understand the mathematics behind the cube, we must first explain the cube and some terminology related to it.

Within the Rubik's Cube world, there are a few terms one must know in order to understand the following work. Fist, one must understand that the cube is made of 26 individual cubies (or pieces). These cubies come of three different styles: the centers, the edges, and the corners. The 6 center cubies are fixed on each face of the Rubik's Cube and consist of only one color. The 12 edge pieces are at crosses from the center and consist of two colors. The 8 corner pieces are located at each corner of the cube and consist of three colors. Each cubie with the exception of the center piece can be described by its location and its orientation. The location is described by the particular space it fills and its orientation is the way it is turned within that space. With all of these terms, one can describe the static state of the cube.

To describe the dynamic state of the cube, we must understand the different types of movements. The most basic movement is a clockwise rotation of a certain face. The second type of movement is a counterclockwise movement of a certain face. The only other type of movement is a double rotation of a certain face (clockwise or counterclockwise does not matter since each yield the same result). We will denote the first type of movement as shown in Figure 1.

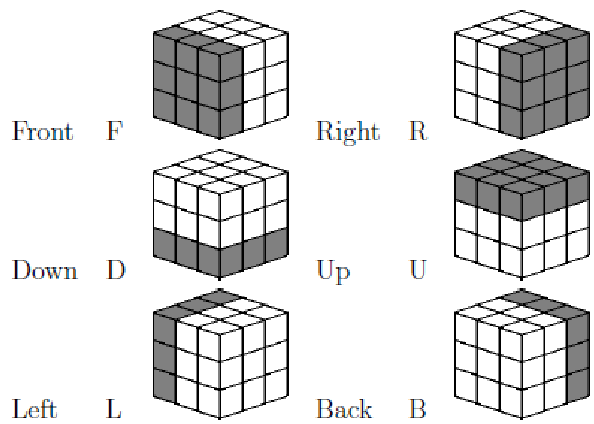

FIGURE 1. Types of Movements [2]

The counterclockwise movements will use the face label shown above for the face followed by prime (i.e. X'). A double rotation will be shown by the face label followed by a squared (i.e. X^2). To concatenate multiple of these moves, we will simply write them together as shown in this example: $RUR'ULDL'U^2$. We will call such concatenation of movements an algorithm. With this, we have the information needed to begin an understanding of the group nature of the Rubik's Cube.

3. The Rubik's Group

Before looking at its group nature, we will first observe the total number of possibilities given by the cube.

EXAMPLE. The number of possible positions of the whole cube can be described by understanding each type of piece. The equation for the number of combinations is

$$\frac{8! * 3^8 * 12! * 2^{12}}{3 * 2 * 2}.$$

In this equation, we know there are 8 positions for corner pieces which can each have 3 possible orientations, so $8! * 3^8$. We have 12 positions for edge pieces which can have two different orientations, so $12! * 2^{12}$. The center pieces are fixed so we need not worry about them. Due to several properties of the cube, we can divide out a 3 and two 2's. This is because there are only certain combinations that are possible with the cube. When these values are divided out, we obtain a final answer of $4.3252 * 10^{14}$ different possibilities with only one correct solution. This yields a random probablility of a $2.312 * 10^{-13}$ % chance of randomly obtaining the solution. ■ [2]

In order to show the Rubik's Cube follows any type of group theory, we must first show that it is in fact a group. We will call this group the Rubik's Group and denote it by $\mathcal{R}$. Recall a group is defined by closure, associativity, and the existence of an identity element and an inverse.

Proof. In order for $\mathcal{R}$ to be a group, it must follow the four properties of a group:

(1) **Closed:** Since any movement possible on the cube still results in the same cube, it is clear $\mathcal{R}$ is closed under the concatenation of the movements defined above. Therefore $\mathcal{R}$ is closed.
(2) **Associative:** Any set of movements can be grouped in anyway one would like without changing the final outcome. Therefore $\mathcal{R}$ is associative.
(3) **Identity:** The identity element is clear: not moving at all (i.e. the empty set) since it will not change the cube. Therefore, $\mathcal{R}$ has an identity.
(4) **Inverse:** The proof of the existence of an inverse is derived from the socks and shoes property. This property says $(ab)^{-1} = b^{-1}a^{-1}$. This applies to the cube since the inverse of any set of movements is the prime movements in the reverse order (i.e. $(RUL'U)^{-1} \to U'LU'R'$). Therefore, $\mathcal{R}$ has an inverse.

Since $\mathcal{R}$ has these four properties, $\mathcal{R}$ is a group. [2]

$\square$

Since we now know that the Rubik's Cube does in fact represent a group, we know that it follows the properties of a group. Since many groups consist of different permutations, is it possible the Rubik's Cube also consists of permutations. Indeed, any set of movements of the cube can be represented as a permutation. These permutations can be created by some algorithm, a concatenation of movements. These algorithms can be represented by a some permutation that shows the movements of each cubie affected by the algorithm. The concept of an algorithm as represented by permutations is shown below.

Let the cubie on the up-front edge be represented by UF. Follow this pattern for all other edge pieces. Let the cubie on the up-front-right corner be represented by UFR. Follow this pattern for all other corner pieces. A permutation P of some algorithm can be shown by ordering each cubie into a cycle permutation as shown in the example.

EXAMPLE. The algorithm $FFRR$ can be represented by the permutation

$$\text{(DF UF)(DR UR)(BR FR FL)(DBR UFR DFL)(ULF URB DRF).}$$

This permutation says the DF cubie will move to the UF space; the UF cubie will move to the DF space. The same for the second set. The sets of three show the BR cubie will move to the FR space; the FR cubie will move to the FL space; the FL cubie will move to the BR space.

Since this permutation consists of two 2-cycles and three 3-cycles, it can be seen that if the permutation (the algorithm) is performed twice, the two 2-cycles will be back to the original positions, and only the three 3-cycles are affected. Similarly, if the permutation is conducted three times, the net change is only the switch from the two 2-cycles. But if the permutation is conducted six times, every piece has returned to its original position. This is represented mathematically by Ruffini's 1799 theorem that the order of a permutation equals the least common multiple of the lengths of each cycle. In this case, $LCM(2, 2, 3, 3, 3) = 6$. So six repetitions of the permutation (algorithm) yields the original position. ■ [1]

An important application of this example is to note that a permutation, if repeated enough times, will return back to its original position. The proof for this statement with reference to the Rubik's Group is below. (Note that this proof references the solved state, but it is easily shown that it applies for any state of the cube.)

Proof. Let P be any permutation of moves in $\mathcal{R}$. Let P^0 equal the solved state, P^f equal the final solved state, P^k equal the state of the cube after k iterations, and let P^m equal the state of the cube after m iterations. We define these so $k < m$ and m is the first time such that $P^k = P^m$. By showing $k = 0$ we will know $P^m = P^f$.

If $k = 0$, we have $P^k = P^0 = P^m$, so $m = 0$ and we are done. If $k > 0$, applying P^{-1} to both P^k and P^m gives the same result since they are both the same position. So $P^kP^{-1} = P^mP^{-1}$ and $P^{k-1} = P^{m-1}$. We defined m as the first time a position would be repeated, with $k > 0$ so the later statement can not be true. Therefore, by contradiction, k can not be greater than 0. Therefore, the first repeat position seen will be $P^f = P^0$. [2] $\square$

This knowledge of permutations can then be extended to determine the number of times any given algorithm must be repeated to obtain the original position. The idea of this concept is that if one can know the permutation representation of any given algorithm, the number of iterations needed to obtain the original position is simply the least common multiple of all of the lengths of each cycle, as shown in the above example. The issue with this comes from a lack of a closed form to represent an algorithm by a permutation of its pieces. If one is given an algorithm, one can perform it once to obtain this permutation and can then easily calculate the number of iterations needed, but one must first perform the algorithm and track the pieces. There is not yet a method of translating an algorithm to the cycles it performs.

There is, unfortunately, one more issue with this idea: the orientation of the cubies is not accounted for. The above method only addresses the position of each cubie, not the orientation of each cubie. Considering this, one can think of the two pieces where orientation will affect the outcome: the corners and the edges. As stated in the introduction, the edges have two possible orientations and the corners have three possible orientations. Taking these into account, we know the LCM between each of these is 6 ($LCM(2, 3) = 6$), so the number of iterations calculated above can be, at most 6 times the number. Specifically, it can be that number, 2 times that number, 3 times that number, or 6 times that number.

Another method to address this issue is to be more specific when labeling cubies for the permutation. Rather than labeling each cubie, we can label each facelet. In doing this, we can track the orientation as well as the position, allowing us to take the LCM of these cycle lengths, giving the total number of iterations needed.

4. Conclusion

With this, we have shown that the Rubik's Cube itself is the physical representation of a very unique and complicated group. We have shown the order of this group exceeds 43 quintillion different possibilities. We have shown that any set of movements can be represented by a permutation of those cubies affected by the algorithm. Finally, we showed that using these permutations, we can calculate the number of times an algorithm must be completed to return the cube to the original state.

There are several areas for further study with this topic. The first is to learn why the number of possibilities is divided by 12. This, of course, represents possible theoretical positions of the cube that are not allowed based off the physical constraints of the cube. Where these omissions come from is a topic of further study. Another topic of further study has not yet been shown: how to provide a set of permutations to represent any algorithm. With this, the algorithms necessary to move certain pieces would be greatly simplified. The other topic of further study has also not yet been proven. It has been shown by brute force calculation that the maximum number of moves required to solve a cube in any given position is 22 moves. [2] Why this number has not yet been proven, but its answer certainly lies somewhere within the group nature of the cube.

There is of course one more topic of further study for any reader. That is how to solve this seemingly impossible puzzle. With 43 quintillion possible combinations, no one can argue the fact that it is a true feat to solve the complexity of this toy that has puzzled mankind for generations.

References

[1] Davis, Tom. "Group Theory via Rubiks Cube." Geometer. 6 Dec. 2006. Web. 10 Dec. 2015.
[2] Li, Jing, and Melissa Gymrek. "The Mathematics of the Rubiks Cube." MIT.edu. 17 Mar. 2009. Web. 10 Dec. 2015.
[3] "The History of the Rubiks Cube." Rubiks. Rubik's Brand Ltd. Web. 10 Dec. 2015.