# The Rubik's Cube Group

Miguel André Brito (106453)

## Abstract

The Rubik's Cube offers a tangible application of Group Theory, serving as a complex model of permutations and orientation. This paper defines the puzzle's operations as a group of transformations. Beyond basic mechanics, we analyze the cube's valid state space and establish the invariant properties of the Rubik's Cube group. The analysis concludes by deriving the exact order of said group, demonstrating how these restrictions reduce the total number of possible permutations.

## 1 Introduction

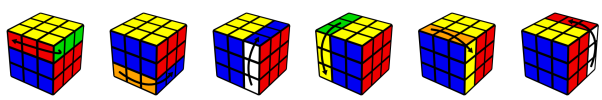
The Rubik's Cube was first introduced in 1974 by Ernő Rubik, a Hungarian architecture professor who initially referred to his invention as the Magic Cube. Geometrically, this puzzle consists of six faces, each with nine smaller squares. While it has been produced in various configurations, the standard 3x3x3 version is by far the most popular and will be the focus of this study. The configuration of the cube is modified by rotating its faces around internal axes, resulting in intricate color permutations. The objective is for the solver to return the cube to its original state: the solved cube where each face displays a single color.

## 2 Move Notation

The cube's possible set of moves can be described by imagining that our cube is laying flat on a surface. Then we simply list out every operation we can legally apply on the puzzle. The cube has 6 different faces which can all be rotated independently one at a time. As such we can define the set of generators of transformations to our cube:

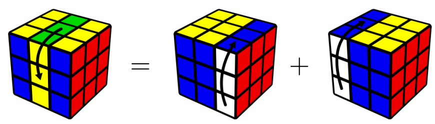
$$S = \{U, D, R, L, F, B\}$$

$U$ : turns the top face clockwise
$D$ : turns the bottom face clockwise
$R$ : turns the right face clockwise
$L$ : turns the left face clockwise
$F$ : turns the front face clockwise
$B$ : turns the back face clockwise



$U$ $D$ $R$ $L$ $F$ $B$

For a transformation $T \in S$, by convention, a face rotation on the clockwise direction is defined as $T$ and its counterclockwise counterpart $T'$. From this generating set we can also create further combinations that turn out to be extremelly useful in solving a scrambled cube. For example, it's very intuitive that we can rotate the middle layer with a move $M$. But we could also achieve the same transformation by rotating the right face clockwise and then the left face counterclockwise, so $RL'$. As such, moves can combine to perform very specific permutations. These operations are called algorithms and they are crucial to effectively solve a scrambled rubik's cube.



$M$ $R$ $L'$

As $T$ represents a 90 rotation it is also useful to point out that $TTT = T'$. We can also define an identity transformation $E = T^4$, which would be the same as not touching the cube. If we'd want to perform the inverse of an algorithm, let's say $T_1 \cdot T_2$, $T_1, T_2 \in S$, we'd have to apply first $T_2^{-1}$ (since $T_2$ was the last transformation) and then $T_1^{-1}$, so $T_2^{-1} \cdot T_1^{-1}$.

## 3 Rubik's Cube Group

Any position of the cube can be described as a permutation of pieces, which means that it is possible that we can describe these transformations as a permutation group. Let $(G, \cdot)$ be the Rubik's Cube Group such that the elements are all possible moves and two moves are considered the same if the final cube state is the same. For a $g_1 \in G$ and $g_2 \in G$, the operation $g_1 \cdot g_2$ is defined as the transformation that applies $g_1$ and then $g_2$ after. We prove that it is a group if it satisfies the 4 properties:

**Closure:**
if $g_1$ and $g_2$ are moves allowed in the cube, $g_1 \cdot g_2$ must be a move as well, so $g_1 \cdot g_2 \in G$ $\checkmark$

**Associative:**
let $g_1, g_2, g_3 \in G$.
$g_1 \cdot (g_2 \cdot g_3)$ and $(g_1 \cdot g_2) \cdot g_3$ both apply $g_1$ then $g_2$ then $g_3$. So $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3,\ \forall g_1, g_2, g_3 \in G$ $\checkmark$

**Identity:**
$\exists\, E \in G$ (as we have previously defined) such that applying $E$ is the same as not touching the cube. So it stands that $E \cdot g_1 = g_1\ ,\ \ g_1 \in G$ $\checkmark$

**Inverse:**
$\exists\, x^{-1} \in G$, such that $x \cdot x^{-1} = x^{-1} \cdot x = E$. As we have established before:

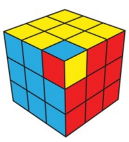
$$x^{-1} = x \cdot x \cdot x, \forall x \in G$$
$$(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}, \forall g_1, g_2 \in G \qquad \checkmark$$

Since executing the same sequence of moves in a different order can result in a different state, this group is a non-abelian.

## 4 Configurations

It is a wrong assumption to say that the possible states of Rubik's cubes is simply the result of permutation of every matching piece with each other. There are legal and illegal configurations, which is to say, cube states that are possible without rearranging the individual pieces and the ones that you can only get after outsmarting (taking apart) the puzzle.

To maintain the integrity of the cube, not all permutations of $S_{54}$ are possible. The center piece on each face is fixed, meaning that as long the cube is handled as intended, the colors of a solved cube will always maintain their original neighboring colors in the same arrangement. As a result the edge piece can only permute with another edge piece in a way that maintains its initial color orientation. For the corner piece the same logic is applied: it can only be sent for another corner piece while maintaining its orientation. Each corner piece can have three different orientations while each edge cubie can only have two. Hence, $G$ is only a subset of $S_{54}$ and not isomorphic to the full permutation group.



[Example of an impossible configuration of a disoriented corner.]

So, the Rubik's Cube is described by the 4-tuple $(s_c, \sigma_c, s_e, \sigma_e)$ where:

- $s_c \in (\mathbb{Z}/3\mathbb{Z})^8$: corner color orientation;
- $\sigma_c \in S_8$: permutation of corner pieces;
- $s_e \in (\mathbb{Z}/2\mathbb{Z})^{12}$: edge color orientation;
- $\sigma_e \in S_{12}$: permutation of edge pieces.

However, not all of these configurations are valid. Valid configurations must respect the first and second fundamental theorem of cube theory.

### I. Theorem of Cube Theory

Let $s_c \in (\mathbb{Z}/3\mathbb{Z})^8$, $\sigma_c \in S_8$, $s_e \in (\mathbb{Z}/2\mathbb{Z})^{12}$, and $\sigma_e \in S_{12}$. The 4-tuple $(s_c, \sigma_c, w, s)$ corresponds to a possible arrangement of the cube if and only if:

(1) $sgn(\sigma_c) = sgn(\sigma_e)$
(equal parity of permutations)

(2) $s_{c_1} + s_{c_2} + s_{c_3} + \cdots + s_{c_8} = 0 \pmod 3$
(conservation of the total number of corner twists)

(3) $s_{e_1} + s_{e_2} + s_{e_3} + \cdots + s_{e_{12}} = 0 \pmod 2$
(conservation of the total number of edge flips)

### II. Theorem of Cube Theory

An operation of the cube is possible if and only if the following are satisfied:

(1) The total number of edge and corner cycles of even length is even.

(2) The number of corner cycles twisted right is equal to the number of corner cycles twisted left (up to modulo 3).

(3) There is an even number of reorienting edge cycles.

## Order of the group

Knowing which configurations are valid, we can compute the order of the group:

$$|\mathbb{G}| = \frac{12! \times 8!}{2} \times \frac{3^8}{3} \times \frac{2^{12}}{2} \qquad (3)$$

Where $|S_{12}| = 12!$, $|S_8| = 8!$, $|(\mathbb{Z}/3\mathbb{Z})^8| = 3^8$ and $|(\mathbb{Z}/2\mathbb{Z})^{12}| = 2^{12}$.

## References

Lindsey Daniels. Group theory and the rubik's cube. *Lakehead Universityc*, 2014.