

# Group Theory and the Rubik's Cube

David Hughes & Grace McNicholas  
National University of Ireland, Galway



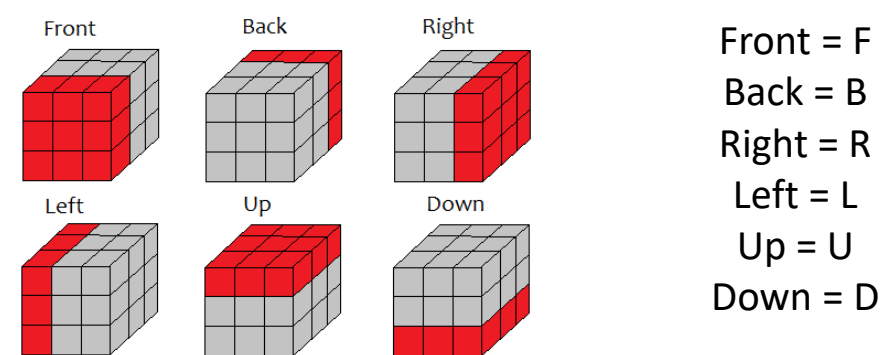
## The Rubik's Cube: A brief history

As many may know the Rubik's Cube is a 3-D puzzle, sometimes referred to as a twisty puzzle. The puzzle was invented in 1974 by Hungarian architect and sculptor Ernő Rubik, and consists of 6 faces containing 9 squares on each face. The aim of the puzzle is to attempt to return a scrambled puzzle to its original state, each side being a single colour. The cube's popularity exploded in the 1980's, and as of 2009 there are estimated to be over 350 million cubes sold worldwide making it the most popular puzzle toy of all time.

## Show the Rubik Cube is a group

When beginning to research this project, we wanted to focus primarily on exploring the effects that the orientation and permutations have on the amount of moves it takes to solve a cube scrambled using a specific algorithm (order). However, we felt it most appropriate to first convince readers that all possible rotations of the Rubik's Cube can be in fact viewed as a group. We can call this  $(G,*)$ .

As we know to be a group must satisfy the following criteria under some binary operation  $*$  to be a valid group:  
A group must be **closed** under the operation  $*$   
A group must contain its own **identity**  
A group must contain the inverse of every move within the group.  
A group must be **associative** under the the operation  $*$



Front = F  
Back = B  
Right = R  
Left = L  
Up = U  
Down = D

We will first take a look at the cube and define the rotations that a Rubik's cube can make. Above we can see U, B, L, F, R, D, which are defined as an 90° clockwise twist, with U, B, L, F, R, D denoted which side of the cube we are twisting. The inverses of each twist U, B, L, F, R, D are given as  $U', B', L', F', R', D'$ , meaning a twist 90° anticlockwise. Using notation we will begin to prove each of the four properties required for this to be a group.

### Identity:

The identity element for an group is an element that when under the binary operation  $*$  does not effect on any other element in the group which it may be joined with under  $*$ .  
In the case of the Rubik's cube, there must exist some element  $I$  such that that when combined with some possible move/series of moves ( $M$ ) it will yield  $M$  again.

$$\Rightarrow M * I = M$$

Therefore, the identity element  $I$  for a Rubik's Cube is when no rotation is completed

$\therefore (G,*)$  has an identity element

### Closure:

$(G,*)$  is defined as the group of all possible rotations under the binary operation  $*$ . So for example, the combination of any two rotations of the cube under the binary operation  $*$ , is the same as making one rotation followed by another rotation.

Using this logic we define  $R_1$  as rotation one and  $R_2$  as rotation two, so  $R_1 * R_2$ .

### Inverse:

The inverse of any rotation of the cube  $R$  can be easily given as the same rotation in the opposite direction  $R'$ . For example, the inverse of the move  $U$  can be given as  $U'$ .

$\therefore (G,*)$  contains the inverse of every element

### Associativity:

To prove associativity, we should first consider three rotations  $R_1, R_2$  &  $R_3$ . These are obviously elements of  $G$ . However to prove that  $G$  is associative we need to show that:

$$(R_1 * R_2) * R_3 = R_1 * (R_2 * R_3)$$

So for example if we had an oriented square ( $S$ ) on the one of the faces of the cube performing the rotation  $R_1$  will move  $S$  to  $R_1(S)$ . if we then performed  $R_2$  it would hence move  $S$  to  $R_2[R_1(S)]$ .

$$\Rightarrow R_2 [R_1(S)] = (R_1 * R_2)(S)$$

Furthermore, we could say that applying the rotation  $R_3$  to  $R_2[R_1(S)]$  (the position of  $S$  after the first two rotations), we will yield  $R_3[R_2[R_1(S)]]$ .

$$\Rightarrow R_3[R_2 [R_1(S)]] = [(R_1 * R_2) * R_3](S)$$

This can also be applied if we were to rotate in a different order namely  $R_2$  first followed  $R_3$ . This would imply that:

$$[(R_1 * R_2) * R_3](S) = [R_1 * (R_2 * R_3)](S)$$

$$\therefore (R_1 * R_2) * R_3 = R_1 * (R_2 * R_3)$$

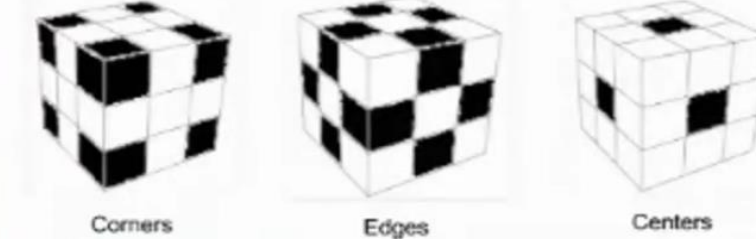
### Conclusion:

The rotations of a Rubik's cube satisfy the characteristics need to be considered a group.

$\therefore (G,*)$  is a group

## Subgroups of Rubik Cubes

The **subgroups** of the Rubik's cube can be seen below: The **corner pieces**, the **edge pieces** and the **centre pieces**. The subgroups that we are interested in in this exploration of the topic edges pieces and the corner pieces. These are going to be important for the next part and also the main part of o



## Orientation vs Permutation: Relationship to the order of a given algorithm

When contemplating an angle to tackle the Rubik's Cube and group theory we decided to take a specific interest in how we might use the subgroups of the cube (edge and corner pieces) to calculate the potential amount of moves that it takes to solve a cube given that we know the algorithm that scrambled it. Having decided this, we began to focus on the orientation and permutation of certain subgroup and the effects that this has on the order of a given algorithm that is needed to return a scrambled cube to its solved state.

Before we continue with individual examples we will first define what we mean by algorithms, orientation, permutation and order in relation to the Rubik's cube:

### Algorithm:

An algorithm is defined as a group of rotations or moves that are used to scramble a solved cube. An example may be as follows:

$$R * U * R' * U * R * U_2 * R' * U$$

This algorithm can be repeated again and again, and will eventually return to a solved state. Our agenda is to use a cube scrambled once to calculate the number of repeated algorithms needed to return it to a solved state.

**Orientation:** Orientation in relation to the cube refers to the different possible ways that each subgroup on the cube can be facing. For example, each corner has three possible orientations, while each edge piece has two possible ways it can be oriented. This important as it allows us to calculate the total possible permutations of a cube, but it will also aid us in discovered the number of repeats of a given algorithm it takes to return a cube to a solved state.

**Permutations:** The number of possible permutations of the faces of a Rubik's cubes is just over 43 quintillion. This enormous number is calculated by calculating the permutations and possible orientations of both the corner and the edge pieces. (The centre piece are stationary and do not need to be considered.)

**Corners:** There are 8 corners on a cube therefore there is  $8!$  (40,320) ways to arrange the corner cubes. Each corner has three possible orientations, although only seven (of eight) can be oriented independently; the orientation of the eighth (final) corner depends on the preceding seven, giving 37 (2,187) possibilities.

**Edges:** There are  $12!/2$  (239,500,800) ways to arrange the edges. Eleven edges can be flipped independently, with the flip of the twelfth depending on the preceding ones, giving 211 (2,048) possibilities.

Using the orientation and permutations of both the corner and edge pieces we can conclude:

$$(8!)(3^7)(2^{11})(12!/2) \approx 43 \text{ quintillion}$$

**Order:** The order of an algorithm refers to the amount of times that a certain set of rotations must be completed in order to return a cube to its solved state. The order of an algorithm is calculated by analysing the changes in orientation and permutation that an algorithm creates. The order of an algorithm is defined as:

$$LCM = [(\text{Length of corner cycle } m \times C_m), (\text{length of edge cycle } n \times E_n)]$$

For all,  $m, n \geq 1$

With the length of the cycle of both the corners and the edges being the amount of both edges and corners that have been permuted.  $C_m$  and  $E_n$  refer to the orientation convention. The orientation convention of the corners of a cube refers to the number of "twists" it will take to return a corner to its correct orientation. This will always be mod 3, as there are three faces to a corner so there will never be more than 3 "twists" to return a corner to its correct orientation.

The orientation convention of the edges of a cube refers to the number of "flips" it will take to return an edge to its correct orientation. This will always be mod 2, as there are only two faces to an edge so there will never be more than 2s "flip" to return a corner to its correct orientation.

## Let's calculate the order of an algorithm

For this we are going to the following algorithm which scrambles the cubes as seen below:

Algorithm:  $R U B' U' R' U R B R'$



This algorithm scrambles the cube significantly with a lot of orientation and permutation changing. To calculate the amount of times we must repeat this algorithm to return the cube to its solved state, we must analyse all the corner and edge pieces that changed orientation and permutation. As we can see from the above cube there are 3 corner pieces and 3 edge pieces that have whose orientation or/and permutation has changed in some way.

Let us first focus on the corner pieces that have permuted. The length of this cycle is 2. The orientation convention will be 3 as it will take 3 more repetitions of the algorithm to return each corner to its correct orientation.

Let us now consider the edge pieces that have permuted. The length of this cycle is also 2. The orientation convention will be 2 as it will take 2 more repetitions of the algorithm to return each edge to its correct orientation.

Finally, we will consider the corner and edge that changed orientation but did not permute. So since they both did not permute the cycle length is one and the orientation convention is 3 and 2 respectively.

If we fill this it to the definition of the order of an algorithm (as seen above) we find:

$$LCM = (2(3), 2(2), 1(3), 1(2))$$

$$\Rightarrow LCM = (6, 4, 3, 2)$$

$$\Rightarrow LCM = (6, 4, 3, 2) = 12$$

Therefore, the order of the algorithm is 12, so it will take 12 repetitions of the algorithm to return the cube to a solved state.

## Interesting Note

As we know from Lagrange's Theorem, if  $G$  is finite set and  $H$  is subgroup of  $G$ . then the order of  $H$  divides the order of  $G$ . this applies to the order of  $G$  and the above example.

$$\frac{43,252,003,274,489,856,000}{12} = 3,604,333,600,000,000$$

## References

- <https://math.stackexchange.com/questions/3357124/how-to-find-the-order-of-a-rubiks-cube-algorithm>
- [https://www.youtube.com/watch?v=RVWtFAcl12k&feature=emb\\_err\\_woyt](https://www.youtube.com/watch?v=RVWtFAcl12k&feature=emb_err_woyt)
- <https://en.wikipedia.org/wiki/Rubik's-Cube-group>