The mathematics of Rubik's Cube

Michael Hutchings

Department of Mathematics
University of California, Berkeley

BAMC Colloquium
UC Berkeley
December 11, 2022

Elements of Rubik's cube

The cube contains:

- six center pieces which do not move relative to each other.
- twelve edge "cubies" each with two stickers on them.
- eight corner "cubies" each with three stickers on them.

The goal of the puzzle is to move all of the edge cubies and corner cubies into their correct positions with their correct orientations.

"It was a big challenge for me. Back then there were no solution manuals or YouTube tutorials, and I was on my own... I knew that a solution existed in theory, but I wasn't sure if one could actually solve the cube in practice.... It was hard and took me a long time – several weeks, that's for sure."

— Ernő Rubik on solving the cube for the first time (*Der Spiegel*, 2010)

Warmup questions

1. If you disassemble the cube, how many ways are there to reassemble it (placing the cubies in any positions and orientations)?
2. If you randomly reassemble the cube, what is the probability that it can be solved (without disassembling it again)?

Answers

1. If you disassemble the cube, how many ways are there to reassemble it (placing the cubies in any positions and orientations)?

12! ways to permute the edge cubies
8! ways to permute the corner cubies
2^{12} ways to orient the edge cubies
3^8 ways to orient the corner cubies
Answer $= 12!8!2^{12}3^8 = 519,024,039,293,878,272,000$

2. If you randomly reassemble the cube, what is the probability that it can be solved (without disassembling it again)?

Answer $= 1/12$
Proof???

Procedure for solving the cube

A typical cube solving procedure:

1. Solve the lower two layers of the cube. (There are various clever tricks to speed this up.)
2. Orient the cubies in the top layer, so that the top face of the cube is the correct color.
3. Permute (i.e. interchange) the cubies in the top layer so that they are in their correct positions.

(To do this fast requires memorizing many shortcuts for dealing with various cases.)

- Fun fact: The cube can always be solved using at most 20 face turns (proved by computer). (Human solves usually need 50-60 turns.)

Goal of this talk

Our goal is to introduce some mathematical ideas with which one can solve Rubik's cube (and other similar puzzles such as larger cubes and other shapes), not so fast, but *understanding each step*.

- The moves that one can perform on Rubik's cube form a mathematical structure called a group.
- One can solve Rubik's cube using two basic ideas from group theory: commutators and conjugation.

Some notation

Basic moves on Rubik's cube:

- F = rotate the front face one quarter turn clockwise
- B = rotate the back face one quarter turn clockwise
- U = rotate the top face one quarter turn clockwise
- D = rotate the bottom face one quarter turn clockwise
- R = rotate the right face one quarter turn clockwise
- L = rotate the left face one quarter turn clockwise

Additional moves (which move the center pieces):

- F_s = rotate a vertical "slice" one quarter turn clockwise as viewed from the front.
- U_s = rotate a horizontal "slice" one quarter turn clockwise as viewed from above.
- Similarly B_s, D_s, R_s, L_s.

Combining moves

If X and Y are two moves on Rubik's cube, then:

- XY means "do X, then do Y".
- $X^2 = XX$ means "repeat X twice". For example, U^2 means rotate the top face a half turn.
- $X^3 = XXX$ means "repeat X three times". And so forth.
- 1 denotes the move of *doing nothing*. This move is called the identity.
- Two moves are considered to be equal if they have the *same effect* on the cube. For example, $U^4 = 1$.

We can think of XY as a kind of "multiplication" of X and Y.

Warning

The usual convention in mathematics would be that XY means do Y first, then do X.

Inverses

- If X is an move on Rubik's cube, then X^{-1} means *undo* the move X. This is called the inverse of X. For example, U^{-1} means rotate the top face a quarter turn counterclockwise.
- To undo a sequence of moves, in general one must undo the moves *in reverse order*:

$$(XY)^{-1} = Y^{-1}X^{-1},$$

$$(X_1X_2\cdots X_n)^{-1} = X_n^{-1}\cdots X_2^{-1}X_1^{-1}.$$

"The inverse of putting on your socks and then putting on your shoes is to take off your shoes and then take off your socks."

- Note that $(X^{-1})^{-1} = X$.

Multiplication is not commutative!

Recall that the usual multiplication of numbers is commutative, e.g. $3 \cdot 5 = 5 \cdot 3$. However:

Important fact

If X and Y are two moves on Rubik's cube, then it is possible that

$$XY \neq YX.$$

In this case we say that "X and Y do not commute".

For example, $FU \neq UF$. (Try it on the cube and see.)

Note

Some pairs of moves do commute. For example $UD = DU$.

We can use noncommutativity to help solve the cube...

Commutators

- If X and Y are two moves on Rubik's cube, their commutator is the move $XYX^{-1}Y^{-1}$, which we denote by $[X, Y]$.

Basic fact

$[X, Y] = 1$ if and only if X and Y commute.

Proof: $[XY] = (XY)(YX)^{-1}$, which equals the identity when $(YX)^{-1}$ is the inverse of XY, i.e. when $YX = XY$.

- Thus the commutator of X and Y measures the *failure* of X and Y to commute.
- Commutators are a very useful tool for solving the cube, as we will now see.

Commutator example 1: Flipping two edges

To flip the top left and top front edges:

1. $X = LU_s^{-1}L^2U_s^2L$ flips the top left edge without disturbing the rest of the top layer. (Here $LU_s^{-1}L^{-1}$ takes the top left edge off the top layer, and then $L^{-1}U_s^{-1}L^{-1}$ puts it back a different way so that it gets flipped.) The lower two layers of the cube are messed up.
2. $Y = U$ moves the top front edge into the top left position, and does not affect the lower two layers of the cube.
3. $X^{-1} = L^{-1}U_s^2L^2U_sL^{-1}$ flips the top left edge (formerly the top front edge) and *repairs the damage to the lower two layers of the cube!*
4. $Y^{-1} = U^{-1}$ now returns the top layer to its original position.

So the commutator

$$[X, Y] = (LU_s^{-1}L^2U_s^2L)U(L^{-1}U_s^2L^2U_sL^{-1})U^{-1}$$

flips the top left and top front edges without disturbing the rest of the cube.

Commutator example 2: Rotating two corners

To rotate the top front left and top front right corners:

1. $X = F^{-1}DFLDL^{-1}$ rotates the top front left corner clockwise without disturbing the rest of the top layer. (Here $F^{-1}DF$ takes the corner off the top layer, and LDL^{-1} puts it back differently so that it gets rotated.) The lower two layers of the cube are messed up.
2. $Y = U$ moves the top front right corner into the top front left position, and does not affect the lower two layers of the cube.
3. $X^{-1} = LD^{-1}L^{-1}F^{-1}D^{-1}F$ rotates the top front left corner (formerly the top front right corner) counterclockwise and repairs the damage to the lower two layers.
4. $Y^{-1} = U^{-1}$ restores the top layer to its original position.

So the commutator

$$[X, Y] = (F^{-1}DFLDL^{-1})U(LD^{-1}L^{-1}F^{-1}D^{-1}F)U^{-1}$$

rotates the top front left corner clockwise and the top front right corner counterclockwise without disturbing the rest of the cube.

“Disjoint permutations” commute

Fact

If X and Y do not affect any of the same cubies, then X and Y commute, so $XYX^{-1}Y^{-1} = 1$.

To understand why, let’s see what happens when we do $XYX^{-1}Y^{-1}$:

1. First do X.
2. Next do Y. This does not affect any of the cubies that were moved by X.
3. So doing X^{-1} moves back all of the cubies moved by X (without affecting the cubies moved by Y). Now it looks like we just did Y.
4. Doing Y^{-1} then brings us back where we started.

For example, $UDU^{-1}D^{-1} = 1$ because U affects only the top layer and D affects only the bottom later.

“Putting on my left shoe commutes with putting on my right shoe.”

Using commutators to permute cubies

Strategy

If X and Y affect few of the same cubies, then they should at least "almost commute", and so $XYX^{-1}Y^{-1}$ should affect only a few cubies. Such a move can be useful if the cube is almost solved.

For example:

Fact

If there is one cubie that is permuted by both X and Y, and if no other cubie is affected by both X and Y, then $XYX^{-1}Y^{-1}$ is a three-cycle, i.e. there are cubies a, b, c such that $XYX^{-1}Y^{-1}$ moves a to b, moves b to c, moves c to a, and does not move anything else.

You can check that this works where:

- a is the cubie moved by both X and Y.
- b is the cubie that Y moves to a. (So Y^{-1} moves a to b.)
- c is the cubie that X moves to a. (So X^{-1} moves a to c.)

Commutator example 3: cycling three corners

- $X = LDL^{-1}$ moves the top front left corner cubie off of the top layer and does not affect the rest of the top layer.
- $Y = U$ affects only the top layer.
- So only the top front left corner cubie is affected by both X and Y.
- By the previous Fact,

$$[X, Y] = (LDL^{-1})U(LD^{-1}L^{-1})U^{-1}$$

is a three-cycle of corner cubies. (It cycles three corner cubies in the front face.)

Commutator example 4: cycling three edges

Let

- $X = R_s$
- $Y = U^2$

Then

$$[X, Y] = R_s U^2 R_s^{-1} U^2$$

cycles three edge cubies: the front bottom, top front, and top back. (This does not quite follow from the previous Fact, but can you see why it works anyway?)

Conjugation

If X and Z are two moves on Rubik's cube, we can make a new move

$$ZXZ^{-1}.$$

This is called a conjugate of X. (Note that this is different from X exactly when X and Z do not commute.)

Intuition

Conjugate moves do the same kind of thing, but in different places.

For example:

- If X flips two edges, then ZXZ^{-1} flips two (usually different) edges.
- If X cycles three edges, then ZXZ^{-1} cycles three (usually different) edges.

Let's see how this works.

Conjugation example 1: cycling three top edges

Goal: cycle the top front, top right, and top left edges.

We know that

$$X = R_s U^2 R_s^{-1} U^2$$

cycles the front bottom, top front, and top back edges. Let

$$Z = F^2 U.$$

What does ZXZ^{-1} do?

1. Z moves the three edges that we want to cycle into the front bottom, top front, and top back positions.
2. X cycles the front bottom, top front, and top back edges (which are now the ones that we want to cycle).
3. Z^{-1} then puts these three edges back where we want them, and repairs any other damage done by Z.

So

$$ZXZ^{-1} = (F^2 U) R_s U^2 R_s^{-1} U^2 (U^{-1} F^2) = F^2 U R_s U^2 R_s^{-1} U F^2$$

cycles the desired three edges on the top face.

Conjugation example 2: cycling three top corners while preserving orientation

Let

$$X = FLF^{-1}, \qquad Y = R^2, \qquad Z = F^2.$$

- The only cubie moved by both X and Y is the front bottom right corner.
- So the commutator $[X, Y]$ is a three-cycle of corners.
- We can check that it cycles the top front rear, front bottom right, and front bottom left corners.
- Z moves the latter two corners to the top layer.
- So the conjugate

$$Z[X, Y]Z^{-1} = F^{-1}LF^{-1}R^2FL^{-1}F^{-1}R^2F^2$$

cycles three corners on the top layer.

This three-cycle is useful if you have already oriented the top layer, because it keeps the top stickers on top.

More conjugation examples

If X is the commutator of two adjacent face rotations, such as $[R, U]$, then X affects four corner cubies and three edge cubies. If Z^{-1} puts all of these on the top layer, then ZXZ^{-1} affects only the top layer. Such moves are useful for orienting the top layer. Examples:

- If $Z = F$ and $X = RUR^{-1}U^{-1}$, then

$$ZXZ^{-1} = FRUR^{-1}U^{-1}F^{-1}$$

  flips two top edges (and rotates two top corners and permutes some top layer cubies).

- If $Z = RU$ and $X = R^{-1}URU^{-1}$, then

$$ZXZ^{-1} = RUR^{-1}URU^2R^{-1}$$

  rotates three top corners (and permutes some top layer cubies).

You can experiment and discover many more!

What we can and cannot do

We have seen how to:

- Do a three-cycle of corner cubies.
- Do a three-cycle of edge cubies.
- Flip two edges.
- Rotate two corners in opposite directions.

It is impossible to do the following (proof???):

- Switch two cubies.
- Flip a single edge.
- Rotate a single corner.

If you disassemble the cube and randomly reassemble it, the probability that it can be solved is

$$\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{12}.$$

Here the first $1/2$ is the probability that you do not have to switch two cubies, the second $1/2$ is the probability that you do not have to flip a single edge, and the $1/3$ is the probability that you do not have to rotate a single corner.

Groups

Definition

A group is a set (collection of objects) G, together with an operation $*$ which inputs two objects in G and outputs a third object in G, such that:

- The operation $*$ is associative:

$$(a * b) * c = a * (b * c).$$

- There is an "identity" object e in G such that for any a in G,

$$e * a = a * e = a.$$

- Every object a in G has an inverse a^{-1} in G such that

$$a * a^{-1} = a^{-1} * a = e.$$

The operation does not have to be commutative: $a * b$ does not have to equal $b * a$.

Examples of groups

- The Rubik's cube group: G is the set of moves on Rubik's cube, $X * Y$ means "do X then do Y", and the identity is the move that does nothing.

This is a rather complicated example. More basic examples:

(1) Various kinds of numbers form groups. For example:

- The set of integers $\mathbb{Z} = \{\cdots, -1, 0, 1, 2, \ldots\}$ is a group with the operation of addition. The identity is 0, and the inverse of n is $-n$.
- The set of nonzero real numbers is a group with the operation of multiplication. Here the identity is 1, and the inverse of x is $1/x$.
- The set of integers mod n is a group with the operation of addition mod n. Here one can think of $G = \{0, 1, \ldots, n-1\}$, and $a * b$ as the remainder when $a + b$ is divided by n.

The above groups are commutative (usually called "abelian").

(2) Groups often arise as sets of *symmetries* of geometric objects. These symmetry groups are often not commutative (nonabelian).

Symmetry group of an equilateral triangle

An equilateral triangle has six symmetries (rotations and reflectons which preserve it):

- $1 =$ identity which does nothing.
- $R_1 =$ rotation which sends vertex 1 to vertex 2, vertex 2 to vertex 3, and vertex 3 to vertex 1.
- $R_2 =$ rotation in the opposite direction.
- $F_1 =$ reflection which switches vertices 2 and 3.
- $F_2 =$ reflection which switches vertices 1 and 3.
- $F_3 =$ reflection which switches vertices 1 and 2.

These form a group, where $X * Y$ means "do X, then do Y".
(Usual mathematical convention would be to do Y first, then X.)
Inverses: $1^{-1} = 1,\ R_1^{-1} = R_2,\ R_2^{-1} = R_1,$
$F_1^{-1} = F_1,\ F_2^{-1} = F_2,\ F_3^{-1} = F_3.$

Symmetry group of an equilaterial triangle, continued

Multiplication table:

	1	R_1	R_2	F_1	F_2	F_3
1	1	R_1	R_2	F_1	F_2	F_3
R_1	R_1	R_2	1	F_2	F_3	F_1
R_2	R_2	1	R_1	F_3	F_1	F_2
F_1	F_1	F_3	F_2	1	R_2	R_1
F_2	F_2	F_1	F_3	R_1	1	R_2
F_3	F_3	F_2	F_1	R_2	R_1	1

From the multiplication table we see that:

- The group is not commutative: $R_1 F_1 = F_2$, but $F_1 R_1 = F_3$.
- R_1 and R_2 are conjugate: $F_1 R_1 F_1^{-1} = R_2$.
- F_1, F_2, and F_3 are conjugate: $R_2 F_1 R_2^{-1} = F_2$ and $R_2 F_2 R_2^{-1} = F_3$.

The group of rotational symmetries of a cube

A cube has 24 rotational symmetries (i.e. rotations which preserve the cube):

- The identity which does nothing.
- Six 180 degree rotations about a line through the centers of two opposite edges.
- Eight 120 degree rotations about a line through two opposite corners.
- Six 90 degree rotations about a line through the centers of two opposite faces.
- Three 180 degree rotations about a line through the centers of two opposite faces.

These form a nonabelian group.
Any two symmetries of the same type (i.e. described by the same bullet point) are conjugate. (Can you see why?)

Permutation groups

Fix a positive integer n. A permutation is a bijection from the set $\{1, \ldots, n\}$ to itself. These from a group where the operation is composition of permutations. (We will continue to write the composition in the nonstandard order, so that fg means "do f and then do g".) This group is the symmetric group, denoted by S_n.
Cycle notation:

- (1 2) denotes the permutation which switches 1 and 2 and leaves all other numbers fixed. In general, a permutation which just switches two numbers is called a transposition.
- (1 2 3) denotes the three-cycle which sends 1 to 2, sends 2 to 3, sends 3 to 1, and leaves all other numbers fixed.

For example:

$$(2\ 3)(1\ 2) = (1\ 2\ 3).$$

In a similar manner, a k-cycle can be written as a product of $k-1$ transpositions.

Even and odd permutations

Any permutation in S_n can be written as a product of $n-1$ or fewer transpositions. (Proof by induction.)

Definition

A permutation is even if it can be written as a product of an even number of transpositions.
A permutation is odd if it can be written as a product of an odd number of transpositions.

- In particular, a k-cycle is an even permutation when k is odd, and an odd permutation when k is even. (Sorry.)
- Any even permutation can be written as a product of 3-cycles. (Exercise using induction.)

Permutation parity is well defined

Theorem

No permutation is both even and odd.

Proof. If f is a permutation, let $\varepsilon(f)$ denote the number of pairs (x, y) of numbers in $\{1, \ldots, n\}$ such that $x < y$ and $f(x) > f(y)$. We can alternately define a permutation to be even when $\varepsilon(f)$ is even, and odd when $\varepsilon(f)$ is odd. Under this definition a permutation is either even or odd but not both. This agrees with the previous definition because composing with a transposition switches the parity of ε. (Exercise)

Back to Rubik's cube

Let G denote the group of operations that one can do on Rubik's cube.

- If one labels the non-center stickers with the numbers $1,\ldots,48$, then one can regard G as a subgroup of S_{48}. (A subgroup of a group is a subset which is closed under the group operation and taking inverses, and thus also a group using the same operation.) This is because every element of G is uniquely determined by how it permutes these 48 stickers.
- If one labels the cubies with the numbers $1,\ldots,20$, then by looking at how an element of G permutes the cubies, we get a homomorphism $G \to S_{20}$. (A homomorphism is a function from one group to another which respects the group structure.)
- Likewise, if one labels the edge stickers with the numbers $1,\ldots,24$, then by looking at how an element of G permutes the edge stickers, we get a homomorphism $G \to S_{24}$.

Proof that one cannot switch two cubies

- Consider the homomorphism $f : G \to S_{20}$ which describes how an element of the Rubik's cube group permutes the 20 cubies.
- If r is a quarter rotation of a single face, then $f(r)$ is the composition of a 4-cycle of corner cubies and a 4-cycle of edge cubies. This is the composition of two odd permutations, hence an even permutation.
- If x is any element of G, then is a product of quarter rotations of faces, so $f(x)$ is an even permutation! Thus $f(x)$ cannot be a transposition.

Proof that one cannot flip a single edge

- Consider the homomorphism $f : G \to S_{24}$ which describes how an element of the Rubik's cube group permutes the 24 edge stickers.
- If r is a quarter rotation of a single face, then $f(r)$ is the composition of two 4-cycles. This is the composition of two odd permutations, hence an even permutation.
- As before, it follows that if x is any element of G, then $f(x)$ cannot be a transposition.

Proof that one cannot rotate a single corner

Definition

A corner labeling is a labeling of each corner sticker with 0, 1, or 2, such that the numbers increase as one goes counterclockwise around the corner.

- Fix a corner labeling. If x is in the Rubik's cube group G, define $f(x)$ to be the total rotation mod 3 of the corners, as measured by the corner labeling. That is, one takes the mod 3 sum, over all corners, of the label of the sticker that is in the '0' position for that corner.
- By definition, $f(1) = 0$.
- Exercise: if r is a quarter rotation of a face, and x is any element of G, then $f(xr) = f(x)$. (This uses the fact that a full rotation of a face does not rotate the corners.)
- It follows that $f(x) = 0$ for all x in G.

A similar argument works for related puzzles such as the Megaminx (the dodecahedral analogue of Rubik's cube).

Subgroups of the Rubik's cube group

Rubik's cube has more puzzles inside it. For example:

- Pick a set of moves (such as $\{R, U\}$ or $\{U^2, D^2, R^2, L^2, F^2, B^2\}$ or $\{U_s, R_s, F_s\}$).
- Mess up the cube using only these moves and their inverses.
- Try to solve the cube using only these moves and their inverses.

Have fun!