Group Theory in a Rubik's Cube

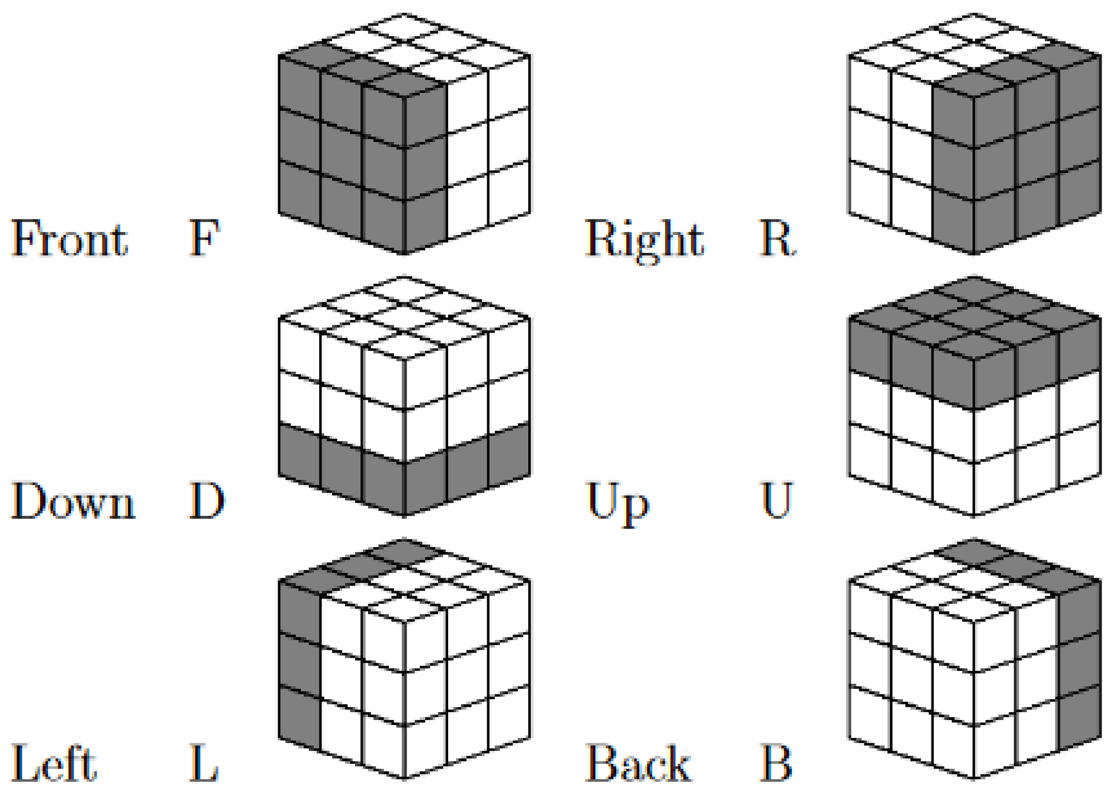
Seán Monahan and Oisín Hodgins

Rubik's Cube

The Rubik's Cube was designed in 1974 by Hungarian sculpter Ernő Rubik. It is a cube with 3x3 squares on every face, each square one of 6 possible colours. With no centre cube, the puzzle consists of twenty-six smaller cubes, referred to as "cubies", with each outward-facing face of a cubie coloured. The space in which a cubie lies is expressed as a "cubicle". The objective of the puzzle is to rotate the sides of the cubes such that every face has only one colour.

How does this relate to Group Theory?

The possible rotations in a Rubiks Cube can be proved to be a group. We can denote the group as $(G, *)$, where G is the set of elements of all possible moves M and $M1 * M2$ is defined as doing the move $M1$ and then $M2$.
The notation of each face as defined by English mathematician David Singmaster, is referred to as Right (r), Left (l), Up (u), Down (d), Front (f) and Back (b). Rotation 90 in the clockwise direction is designated as R,L,U,D,F,B on each respective face, while a rotation in the anti-clockwise direction is similarly denoted as R_i L_i U_i, D_i, F_i, B_i.



The elements of G consist of all possible moves of the Rubik's cube. To prove that the $(G, *)$ is a group, we must prove that each property of a group is fulfilled.

Proof that the Rubik's Cube Group is a Valid Group

Closed Property :
$(G, *)$ is closed under the operation $*$, if $M1$ and $M2$ are operations, and $M1*M2$ is defined as moving $M1$ and then $M2$, then $M1 * M2$ is also a move and is part of $(G, *)$.
Identity Property :
The identity e can be defined as the move that does not perform any rotations. Thus $M1e$ would mean be defined as doing $M1$ and then executing no rotations, so $eM1$ would be the doing nothing and then performing $M1$ which is clearly the same. Therefore, the identity property holds for $(G, *)$
Inverse Property :
If $M1$ is a move, we can define $M1'$ to be the reverse operation of that move, ie., if $M1$ makes the move FU_i then $M1'$ is the move F_iU. Thus every operation M has an inverse.
Associative Property :
Proving associativity is somewhat trickier. First we will let C be an oriented cubie, then we can define $M(C)$ to be the oriented cubicle where C lies after move M.
Then if $M1 * M2$ is the operation where $M1$ is performed and then $M2$ is carried out after, then $M1$ moves C to $M1(C)$ and $M2$ moves C to $M2(M1(C))$.
Then, $(M1 * M2)(C) = (M2(M1(C))$
For $*$ to be associative, $(M1 * M2) * M3 = M1 * (M2 * M3)$
From before we can denote that the operations do the following: $[(M1 * M2) * M3](C)$ and $[M1 * (M2 * M3)](C)$ respectfully.
As demonstrated from before, $[(M1 * M2) * M3](C) = M3([M1 * M2])(C) = M3(M2(M1(C)))$ but also $(M1*(M2*M3))(C) = (M2*M3)(M1(C)) = M3(M2(M1(C)))$
Thus $(M1 * M2) * M3 = M1 * (M2 * M3)$, ie. $*$ is associative.

These 4 characteristics prove that $(G, *)$ is in fact a valid group.

How does Group Theory help us solve a Rubik's Cube?

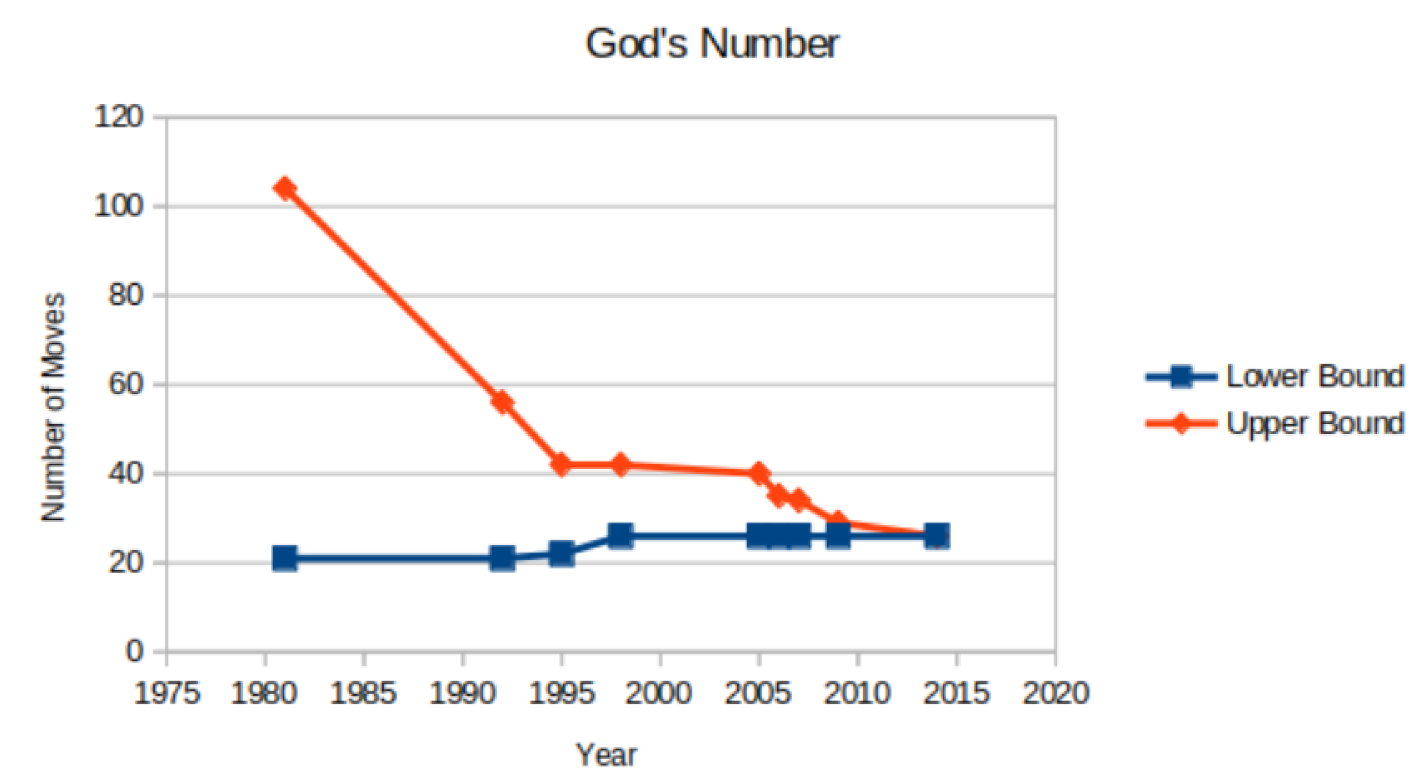
Group theory helps us produce algorithms which can not only solve the rubiks cube but helps us solve it more efficiently, ie. with less moves and less time. This is done by looking at the commutativity of the group.
Commutators :
$(G, *)$ is non-abelian, it does not always satisfy the commutative property $M1 * M2 = M2*M1$. Because of this we can come up with commutators of the form $M1*M2*M1'*M2'$ that carry special functions like flipping an edge and rotating two corners.
Some face rotations do commute, such as U and D. In this case the commutator is $U * D * U_i * D_i$, which clearly commutes as U and D do not directly influence each other.
Commutators are vital for solving the Rubik's Cube as they can be used to carry out specific functions whilst retaining any cubies that are already in the correct position.
Let's show an example of a more complicated commutator, here is how to flip the top right and top front edge:
Let $M1 = RU_iR^2U_i^2R$, $M2 = U$ with $M1' = R_iUR_i^2U^2R_i$, $M2' = U_i$
The commutator here is $M1 * M2 * M1' * M2'$. $M1$ here flips the top right face while retaining the rest of the top layer. $M2$ moves the top front edge into the top right position, while retaining the bottom two layers. $M2'$ flips the top right face and returns the other two layers to their original position. $M2'$ then returns the top layer to its original position.
Conjugates :
Another way that group theory helps with is with Conjugation.
If $M1$ and $M2$ are two moves then the conjugate Z of $M1$ is $Z = M2M1M2'$. The conjugate has the same function as the original move $M1$ but does the move in a different location, as in the example below:
Here we will use conjugations to cycle the bottom three edges.
Let $M1 = R_iD^2RD^2$ $M2 = F^2D$, $M2' = F_i^2D_i$, $M2M1M2' = F^2DR_iD^2RD^2F_i^2D_i$. $M2$ moves the three edges to the front bottom, bottom back and top back positions. $M1$ then cycles these three edges, then $M2'$ returns the edges to their original position, cancelling out any disordering from $M2$. Thus the conjugate of $M1$ cycles the desired 3 three edges without ultimately changing the position of any cubie.

Observations we can find using Group Theory

We can deduce that $(G, *)$ is symmetric due to its permutational operation. The elements of G consist of the 3 orients of the 8 corner cubies and 2 orients of the 12 edge cubies, which is 48 elements in total. Therefore $(G, *)$ must be a subgroup of $S48$. We know it is a subgroup because there are some illegal configurations of the cube that cannot be produced using the standard operations. Intuitively the only way to reach these configurations would be to physically dismantle and reassemble the cube, which of course is against the rules of the puzzle. We can actually calculate the chance that a rubiks cube reassembled at random will be solvable. With corner cubies only one of the three orientations is valid, with edge cubies only one of the two configurations is valid and the parity of the permutation of all edges must remain even. Therefore there is a $1/12$ chance that the Rubik's cube would be solvable.

Cubing, Computers and God's Number

After professor Ernő Rubik first presented his invention, the Magic Cube, to his students at the Bupapest College of Applied Arts in 1974 it was believed that a computer would be needed to solve it! Only after a month of searching was the first solution found, despite the fact that almost every student was searching for one.
In the present day we have many algorithms for solving the Rubik's cube, however up until recently there remained some unanswered questions about the mathematical secrets of this seemingly simple 3x3 cube, ones that mathematicians and indeed the group theorists among them, have been puzzling over for years. One such example is God's number or the minimum number of moves needed to solve from any starting position, it is given the name as no mortal mind could possibly look at any cube and plan a series of optimal moves to solve it! God's number has a long history, beginning in 1981 when Morwen Thistlewaite first proved, using his own algorithm, that 104 moves suffice to solve any of the 43 quintillion different scrambles.
In this area it is important to distinguish between the half-turn metric (htm) and quarter-turn metric (qtm). The htm allows a face to be turned 90,180 or 270 degrees in one go, and that to be counted as a single move, whereas the qtm only counts moves of 90 degrees.
The graph below shows how research on the upper and lower bounds of God's number has developed through the years, and converged to 26, a number proven by Tomas Rokicki and Morely Davidson.



But how did they do it? They used principles of group theory to partition all possible positions into 2,217,093,120 sets of 19,508,428,800 positions each, which was reduced through the group theory principles of symmetry and set covering. They then wrote a program to solve each set in 26 moves or less, which took roughly 17 seconds per set, totalling to roughly 29 years of CPU time at the Ohio supercomputer!
This means no matter what position you find yourself face-to-face with you know that it can be solved in a mere 26 moves or less, not that the human mind could evaluate this set of moves just by looking and planning ahead though.
What is significant about this 26 move maximum however, is the fact that only a single position(and its 2 rotations) has been found so far on the cube requires all 26 moves to solve despite significant effort to find others. It is the superflip composed with fourspot and is shown on the cube in the top right corner of this poster!

References

http://precollegiate.stanford.edu/circle/math/notes07f/group.pdf
https://math.berkeley.edu/ hutching/rubik.pdf
https://en.wikipedia.org/wiki/Rubik's_Cube_group