THE MATHEMATICS OF THE RUBIK'S CUBE

MICHAEL TRAVIS

ABSTRACT. In 1974, the Hungarian architect Ernö Rubik invented the familiar $3 \times 3 \times 3$ Rubik's Cube while teaching at the School for Commercial Artists in Budapest. The cube quickly became a world phenomenon, and many different methods to restore a scrambled cube to its initial, pristine state of 6 solid-color faces were discovered. This paper will not detail such a method; it will, however, describe the group theory embodied in and by the cube as well as its combinatorial properties. Additionally, an interesting analogy to modern physics will shove its head in, as physics so often does.

CONTENTS

1. SOME GROUP THEORY

A *group* is an ordered pair $(G, *)$ with G a set and $*$ a binary operation satisfying:
(i) $(a * b) * c = a * (b * c)$. (associativity of $*$)
(ii) $\exists$ element $1 \in G$ such that $\forall a \in G$, $a * 1 = 1 * a = a$. (existence of identity)
(iii) $\forall a \in G$, $\exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1$. (existence of inverse)

For example, the integers $\mathbf{Z}$ under the binary operation of addition form an *abelian* (meaning the operation is commutative, as well) group, $(\mathbf{Z}, +)$ in which the identity is the 0 element and the inverse of an element z is $-z$. Another example of a group is the set $\mathbf{R}\backslash\{0\}$ under multiplication.

Denote the top, bottom, right, left, front, and back faces of the Rubik's Cube by U, D, R, L, F, B, respectively. Define a *move* X as a 90 degree clockwise turn of face X.

Definition 1.1. The set of all sequences of moves under composition forms the cube group M.

In effect, a sequence of moves is the same as a "scrambling" of the cube.
Associativity holds trivially in this group; the identity is the "move" of doing nothing; the inverse of X, hereforth denoted X', is defined as a 90 degree turn counterclockwise of face X, and clearly $XX' = 1$.

Remark 1.2. To simplify, the middle layer turns will be ignored for the purposes of this paper, as they are effectively the same as turning the outer two sides in opposite directions.

Definition 1.3. A *direct product* of two groups A, B is defined by $A \times B := \{(a, b) | a \in A, b \in B\}$.

2. Permutations

A *permutation* is a bijection from a set to itself. A *cycle* is a subset of a permutation which in which the set of affected elements, E can be ordered and every element of E is sent to another element of E. For example, (1423) is the cycle whose permutation induces $1 \to 4 \to 2 \to 3 \to 1$, and this is called a *4-cycle*, as it has 4 elements; this 4-cycle can be written as (14)(42)(23). A cycle of length 2 is called a *transposition*, and a permutation is called *even* if it can be decomposed into an even number of transpositions, and *odd* if it can be produced by an odd number of transpositions. For example, the above 4-cycle is odd as it decomposed into 3 transpositions; in fact, a cycle of length n can be decomposed into $n - 1$ transpositions. It turns out that any permutation is either even or odd, and the one refers to the sign of an even permutation as $+1$, while the sign of an odd permutation as -1. The following theorem about inverses of elements holds true in *any* group.

Theorem 2.1. $(XY)^{-1} = Y^{-1}X^{-1}$.

Proof. By the properties of a group, $1 = (XY)^{-1}(XY)$, so multiplying both sides on the right by $Y^{-1}X^{-1}$ gives the desired equality. Intuitively, if you rotate the front face then the top face, the way to undo this is to rotate the top face counterclockwise and then the front face counterclockwise. □

2.1. Even Permutations.

Any basic move is a 4-cycle on both corners and edges, or a double 4-cycle: Then it is a product of two odd transpositions and is thus even. Now any move composed upon another move is still even since even times even is even under the group operation of composition. Then only even permutations on the cube can be reached from the solved state. But how many of the total permutations are even?

Theorem 2.2. *Exactly half of the even permutations of the cube are even.*

Proof. Let p be an even permutation. Since $pp^{-1} = 1$, p^{-1} is also even because 1 is even since $p = p1$. An even permutation times an even permutation is still even, so the even permutations form a subgroup of the group of permutations. Now suppose p is odd and q is even, then pq is odd. Define $r = pq$, where r is odd and this is true for any r. Now let $q = p^1 r$ and the map $q \mapsto pq$ is one-to-one and onto from even to odd permutations, so either half are even and half are odd, or all are one or the other. Therefore, half of the total permutations are even. □

3. Group Actions

A *group action* of a group G on a set S is simply a map from $G \times S$ to S defined by gs satisfying:
(i) $g_1(g_2 s) = (g_1 g_2)s$, $\forall g_1, g_2 \in G$, $s \in S$.
(ii) $1s = s$, $\forall s \in S$.
For example, the group $(\mathbf{Z}, +)$ acts on the set of real functions of a real variable with $(gf)(x) = f(x + g)$ with g an element of $(\mathbf{Z}, +)$.

4. Orbits

As defined in section 1, the cube group M is the set of sequences of moves under sequence composition. Now consider the construction of the cube. It is made up of 27 "cubies," one of which remains hidden in the middle. The 6 center face tiles are always in the same position relative to each other, so in effect, there are only 20 relevant cubies, consisting of 12 edge pieces and 8 corner pieces. Call the set of these 20 cubies Λ, and let M act on Λ by the traditional face rotation.

Definition 4.1. An *orbit* of an element, $a \in S$ for S an arbitrary set with a group G acting on it, is the subset of S consisting of the elements of S to which a can be moved by the group action.

Then Λ has two orbits: Λ_e, the edge pieces, and the corner pieces Λ_c. These are orbits because a corner piece can only move to another corner piece, and an edge piece can only be moved to another edge piece by turning a face. Since they are disjoint, $\Lambda = \Lambda_e \cup \Lambda_c$ and $|\Lambda_e| = 12$ and $|\Lambda_c| = 8$ by a simple counting argument.

Now consider the faces of the cube. There are 54 total tiles of color; The 6 center tiles only rotate about their respective axes and remain loyal to their faces. This leaves now 48 tiles. Define the set Δ to be these tiles, with Δ_c the corners and Δ_e the edges. Very similarly to Λ, $|\Delta_e| = |\Delta_c| = 24$ where these are the two orbits of Δ, and $\Delta = \Delta_e \cup \Delta_c$.

5. Cycles

Recall that for faces X, Y, $(XY)^{-1} = Y^{-1}X^{-1}$. Now consider the move $(X^{-1}Y^{-1}XY)$ for X, Y adjacent faces.

Definition 5.1. A *commutator* in a group G is an element of the form $(X^{-1}Y^{-1}XY)$, with X, Y in G, also written as $[X^{-1}Y^{-1}]$ for X, Y elements of the group. Clearly $[X^{-1}Y^{-1}]$ is also in the group by closure.

This move, $[X^{-1}Y^{-1}]$, acts as a 3-cycle on Λ_e: if the edges are numbered 1-12 in clockwise descending order with 1 at the top front and X and Y are the top and right faces, respectively, then $[X^{-1}Y^{-1}]$ creates the cycle (148). In other words, it permutes 3 edges around such that if the move is done 3 times it will be the identity on Λ. Then this move has order 3. On Λ_c, $[X^{-1}Y^{-1}]$ acts as a double transposition

(two disjoint transpositions): if the edges are numbered 1-8 clockwise descending with 1 at the top right, then $[X^{-1}Y^{-1}]$ creates (12)(48).
The commutator acting on Δ, however, is slightly trickier. Number the elements of Δ_e from 1-24 clockwise descending such that 1 is on the top face at the front, 5 is on the front face at the top, 9 is the front face at the right, etc. Then $[X^{-1}Y^{-1}]$ acts on Δ_e as (14[14])(58[15]). A logical numbering of the elements of Δ_c reveals that $[X^{-1}Y^{-1}]$ acts on Δ_c as (197862)(4[20][12][21]5[13]). Hence the commutator acts as a double 6-cycle on Δ_c and a double transposition on Δ_e. Logically one might suppose then that repeating the commutator 6 times might equal the identity on both Λ and Δ, and this, by observation turns out to be true.

Definition 5.2. Consider a permutation, p of the cube. Then the *order* of the permutation p is how many times one must repeat it in order to reach the identity.

For instance, ord(R)= 4 because four rotations of the right face return it to the solved state.

Theorem 5.3. *If p can be written as a product of disjoint cycles: $p = C_1C_2...C_n$ for C_i a cycle, then ord(p) is equal to the least common multiple of the orders of the cycles.*

Proof. If $p = C_1C_2...C_n$, then $p^m = C_1^mC_2^m...C_n^m = 1$ iff $C_i^m = 1$ for all $1 \leq i \leq n$ which is iff m is a multiple of the order of each C_i. Thus ord(p) is the least common multiple of (ord(C_1), ord(C_2), ... , ord(C_n)). □

A simple example of the above theorem is the permutation RU. This sequence cycles 7 edges, 5 corners (but twisting in all 3 ways, hence a 15-cycle), and rotates one corner about itself(a 3-cycle.) Therefore, the order of (RU) is lcm(3, 7, 15)= 105. If you're not pressed for time, you can check this by doing the move RU 105 times and seeing if it is the smallest number that returns the cube to its solved state.

Proposition 5.4. *The 3-cycles created by $[X^{-1}Y^{-1}]$ generate the group A_{12} (called the commutative subgroup) of all even permutations of Λ_e and the group A_8 of all even permutations of Λ_c.*

Proof. A 3-cycle can be produced by two transpositions, so this is an even permutation. Now number each edge on the cube such that the top layer has edges 1-4 with 1 in front, the middle layer has edges 5-8, and the lower layer has edges 9-12 and the numbers helix down clockwise from 1. Treating Y as the top face and X as the right face, $[X^{-1}Y^{-1}]$ creates the 3-cycle (184). Redoing the move to create a 3-cycle with 1 entry in common with (184), such as (398) creates the 5-cycle (13984). This is again an even permutation since it's a cycle of odd length, and this 5-cycle over all possible faces X, Y generates the alternating group along with other combinations of commutator-induced 3-cycles generates A_5. Similarly, adding another 3-cycle with one entry in common creates A_7 over the edges, another generates A_9, one more generates A_{11}, and another to permute the final edge clearly shows that these 3-cycles generate the group A_{12}. This is all keeping in mind the fact that any 3-cycle of edges can be reached via this commutator and its variations (rearranging the order of a commutator keeps it a commutator) and an edge transposition commutator $U^{-1}F^{-1}L^{-1}B^{-1}R^{-1}URBLF$, which is in fact an extension and combination of the commutator and two variations.

On Λ_c, $[X^{-1}Y^{-1}]$ is an even permutation as it is a double transposition. Now consider adding another double transposition of the same move with 1 corner in common to generate A_7. One more double transposition with the final corner finishes the generation of A_8. Once again, any cycle of corners on the rubik's cube can be achieved via this commutator and its variations. □

From this result it is clear that a cube can not be solved if two corner pieces had been switched with each other with all other pieces in their solved state, as that would be an odd permutation. Hence, it is impossible to switch two cubies (keeping the same rotation) and solve the cube. These ideas will be further discussed in the following sections.

6. The Permutation Group P

Let P denote the group of all permutations of Λ induced by M, the cube group. Then the group P consists of all combinations of all edge permutations S_{12} and corner permutations S_8 because one can see that any edge piece or corner piece can be moved to a neighboring space by some sequence of moves. Hence, P is just a subgroup of $S_8 \times S_{12}$.

Definition 6.1. The *parity* of a permutation indicates whether the permutation is even or odd.

Proposition 6.2. $|P| = \frac{1}{2} \cdot 8! \cdot 12!$

Proof. As shown above, P contains $A_8 \times A_{12}$. Now if a move is odd on both Λ_c and Λ_e or even on both Λ_c and Λ_e, then Λ is even. However, every move gives an even permutation of Λ since any move acts as a 4-cycle on both edges and corners. So $(S_8 \times S_{12}) \cap A_{20}$ consists of all these even permutations and has $A_8 \times A_{12}$ as a subgroup of order 2. Then we have shown that $(A_8 \times A_{12}) \leq P \leq (S_8 \times S_{12}) \cap A_{20}$. Then P must consist of all permutations in which Λ_c and Λ_e have the same parity and is equal to $(S_8 \times S_{12}) \cap A_{20}$. Hence, the order of P is $\frac{1}{2} \cdot 8! \cdot 12!$. □

7. The Construction Group C

Consider taking Rubik's Cube apart and reconstructing it however you like such that it stills creates a cube with the familiar 8 corners and 12 edge pieces. Call this group of all possible constructions of the cube C (with the same sequence composition as M) and of course M is a subgroup of C. Now a simple combinatorics argument shows the order of C: There are 8 corners which can be placed in any order with 3 possible orientations each, and 12 edges which can be placed in any order with 2 permutations each. Therefore,

$$|C| = 8! \cdot 3^8 \cdot 12! \cdot 2^{12} \tag{7.1}$$

7.1. **The Wreath Product.**

Definition 7.2. The *kernel* of an action is the set of elements of C that act trivially on every element of Λ: $\{c \in C | c \cdot a = a\}$.

Definition 7.3. If groups A, B are groups of permutations of finite sets C, D respectively, then the *wreath product* $A \wr B$ is defined to be the group of permutations e of the set $C \times D$ which are of the form

$$e : (c, d) \mapsto (c \cdot a_d, d \cdot b) \tag{7.4}$$

where $a_d \in A$ and $b \in B$. So e depends on an element of B and a function from D to A.

Now, observe that C_c, the corner orbit of the construction group, acts on Λ_c, the corner orbit of the cubies as the symmetric group S_8 because one can construct the corners in any order one likes. Additionally, each corner cubie can be rotated through angles $\frac{2\pi k}{3}$ for k an integer. Hence, in these three rotations each cubie represents the cyclic group Z_3 since every non-identity element has order 3, and the direct product of all 8 cubies is a direct product of 8 copies of Z_3. Call this octupal direct product K_c since it is a kernel of the action of C_c on Λ_c.

Similarly, C_e acting on Λ_e is the symmetric group S_{12} and the kernel group K_e is a direct product of 12 copies of Z_2 since each corner can be rotated through angles $k\pi$ for k an integer and every non-identity element has order 2. Both kernel groups are abelian.

The wreath product of Z_3 by S_8 (as a homomorphism from Λ_c) is the semidirect product of K_c by S_8 with respect to the aforementioned homomorphism and is denoted by $Z_3 \wr S_8$. This wreath product is equal to C_c and $C_e = Z_2 \wr S_{12}$. Since C_c and C_e are seperate orbits of C, it follows that

$$C \cong (Z_3 \wr S_8) \times (Z_2 \wr S_{12}) \tag{7.5}$$

Intuitively, this makes some sense because we know the order of C_c and C_e, and these line up easily with the order of the symmetric and cyclic groups. The wreath product essentially describes the way that the corners or edges can be arbitrarily permuted in position and semi-independently oriented.

7.2. **The Orientation Group Ω.** Define the group Ω to be the group consisting of all compound moves that leave the cubes in the original position but not necessarily the original orientation. For instance, a move that rotates 3 corners 1 turn clockwise but leaves them in their original locations is in Ω. Write Ω_c, Ω_e for the groups of permutations induced by Ω on Δ_c and Δ_e, respectively.

Remark 7.6. Since each of these orientation groups is a subgroup of their corresponding kernel groups (as defined above), it follows that they are abelian of orders 3 and 2, respectively.

8. Parity

One way to make a cube impossible to solve is to rotate a single corner piece by $\frac{2\pi}{3}$ radians. We now try to see why this is so.

For any permutation of the cube, add up the clockwise radians each corner cubie has turned from the cubie that was originally there. This sum is an angle of the form $\frac{2\pi k}{3}$ where k is 0, 1, or 2 modulo 3.

Theorem 8.1. *For any permutation of the cube, k=0*

Proof. Define a map $T : C \to (\mathbf{Z}/3\mathbf{Z})^+$ defined as $T(p) = \frac{3}{2\pi}\sum_{i=1}^{8}\Theta_i = k\text{mod}3$ where Θ_j represents the change in angle of the j^{th} corner cubie from the previous corner cubie in that position and p is any element of C. Now suppose p and q are elements of C. Then $T(pq) = \frac{3}{2\pi}\sum_{i=1}^{8}\Theta_{pq_i} = \frac{3}{2\pi}\sum_{i=1}^{8}(\Theta_{p_i} + \Theta_{q_i}) = \frac{3}{2\pi}\sum_{i=1}^{8}\Theta_{p_i} + \frac{3}{2\pi}\sum_{i=1}^{8}\Theta_{q_i} = T(p) + T(q)$, so T is a homomorphism. By easy observation, any of the six basic moves keeps $k = 0$. Therefore, any series of moves and any permutation from the solved state will have $k = 0$. □

A similar proof holds for the edge pieces, which in fact requires that the change in rotation to be of the form $m\pi$ where m is 0 or 1 modulo 2.

8.1. **Quark Theory.** The Rubik's Cube contains an interesting analog to quark confinement.

Definition 8.2. *Color Confinement* states that colored particles, including quarks, can't be isolated. They must occur in either pairs or triplets such that their color (a physical property) remains neutral. As such, no single quark has a neutral color.

Quarks' "color" is represented by fractional electric charges, either $\frac{1}{3}$ or $\frac{2}{3}$. An anti-quark has these same charges but they are negative. Consider a clockwise rotation of a corner to be a positive charge while a counterclockwise twist a negative charge. Then the law above that $k = 0$ is analagous to combinations of quarks. A meson consists of a quark and an anti-quark pair, while a baryon is a combination of three quarks. Any particle made up of quarks (or any particle in the universe) must satisfy the law that its electric charge must be an integral value. Thus, from a solved cube, one can turn corner 1 one twist clockwise, and in order for it to be solvable one must either: turn another corner one twist counterclockwise or two other corners clockwise.

9. The Order of M

Now finally we arrive at the ultimate question of Rubik's Magic Cube: How many possible solvable permutations exist? Keeping in mind what we have gone over so far, it is not too difficult: The edges can be permuted in 12! ways and the corners in 8! but the permutation must be even, so there is a factor of $\frac{1}{2}$. The first 7 corners can each be in 3 different orientations, but the 8th one is restricted to one position since $k = 0$; similarly, the first 11 edges can be in any of 2 positions, but the 12th is restricted to 1 in analog. Hence,

$$|M| = \frac{1}{2} \cdot 8! \cdot 3^7 \cdot 12! \cdot 2^{11} \approx 4.3 \times 10^{19} \quad (9.1)$$

Notice that $|C : M| = |C|/|M| = 12$, which means that if the cube is randomly constructed after being taken apart, there is only a 1 in 12 chance that it will be solvable.

To get a sense of the size of $|M|$, consider rotating a face every second. It would then take 1.4×10^{12} years to get through every single permutation. The universe, by comparison, is about 1.4×10^{10} years old. So if someone ever tells you that they "figured that thing out once; it took forever but [they] finally got it just randomly turning faces," you have a right to be skeptical.

References

[1] David Singmaster. Notes on Rubik's Magic Cube. Enslow Publishers. 1981.
[2] Peter M. Neumann, Gabrielle A. Stoy, and Edward C. Thompson. Groups and Geometry. Oxford University Press. 1994.
[3] David S. Dummit and Richard M. Foote. Abstract Algebra, 3rd edition. John Wiley & Sons. 2004.