GROUP THEORY AND THE RUBIK'S CUBE

HANNAH PROVENZA

Abstract. Here we present a basic introduction to the theory of groups and permutations. Then we will define the group generated by operations on the Rubik's cube, the classic toy invented in 1974 by Hungarian sculptor and architect Erno Rubik that caused a sensation in the 1980s, quickly becoming one of the world's best-selling toys. Finally, we will find the order of the group and explore current research to find its diameter.

Contents

1. Groups

Definition 1.1. A **group** G is a set of points with an operation, $*$, that relates every pair of elements x and y such that the following properties are satisfied:

(1) **Closure**: $\forall x, y \in G, x{*}y = z \implies z \in G$.
(2) **Associativity**: $\forall x, y, z, \in G$, we have $x{*}(y{*}z) = (x{*}y){*}z$.
(3) **Identity**: $\exists$ an element $1 \in G$ such that $\forall x \in G$, $x{*}1 = 1{*}x = x$.
(4) **Inverse**: $\forall\ x \in G$, $\exists x^{-1}$ such that $x{*}x^{-1} = 1$.

Example 1.2. The integers form a group, $\mathbb{Z}$, under addition, in which the identity is 0 and the inverse of each z is $-z$. This group also has the property of **commutativity**, meaning that $\forall x, y \in G, x + y = y + x$. Groups with commutativity are also known as **Abelian** groups. Another example of an Abelian group is the set $\mathbb{R}\backslash 0$ under multiplication. In this case, 0 is excluded because there is no element in the reals that is its inverse.

Definition 1.3. The **center** of a group G, denoted $Z\left(G\right)$, is the set of elements that commute with every other element of G. Another way of expressing this is $Z\left(G\right) = \{z \in G | zg = gz \forall g \in G\}$. A group is Abelian iff $Z\left(G\right) = G$, and a group is centerless iff $Z\left(G\right) = I$.

Date: 10 July 2009.

2. Permutation

Definition 2.1. A **permutation** is an invertible mapping of a finite set $\mathbf{N}$ onto itself. A **cycle** is a subset of a permutation in which the affected elements, E, can be ordered, and every element of E is sent to another element of E. For example, $(1\ 3\ 4\ 2)$ is the cycle whose permutation induces $1 \to 3 \to 4 \to 2 \to 1$. In this example, E has four elements; accordingly, it is known as a 4-cycle.

Theorem 2.2. *Every permutation P of degree n is a product of uniquely defined disjoint cycles.*

Proof. By induction.

The permutation P maps the symbol 1 into p_1, the symbol p_1 into p_{p_1}, the symbol p_{p_1} into $p_{p_{p_1}}$ etc. and finally $p_{p_{\ddots_1}}$ into 1; hence $P = \left(1\ p_1\ p_{p_1} \cdots p_{p_{\ddots_1}}\right) Q$ where Q is a permutation of degree N which does not affect the symbols affected by the uniquely defined cycle $\left(1\ p_1\ p_{p_1}\ \cdots\ p_{p_{\ddots_1}}\right)$, with Q of degree $n-1$ if $p_1 = 1$. We assume the theorem to be correct for all permutations of degree $< n$; thus it is correct also for the permutation P of degree n. $\square$

Definition 2.3. A cycle of length two is known as a **transposition**.

Theorem 2.4. *Every permutation P is a product of transpositions.*

Proof. This follows from Theorem 2.2 when we show that it is true for cycles:

$$(1\ 2\ \dots\ m-1\ m) = (1\ m)\,(1\ m-1)\dots(1\ 3)\,(1\ 2) \tag{2.5}$$

This proof also demonstrates that an n-cycle can be decomposed into $n-1$ transpositions. We should note, however, that these transpositions need not be disjoint. $\square$

Definition 2.6. We say that a permutation is **even** or **odd** if it can be written as the product of an even or odd number, respectively, of transpositions. The evenness or oddness of a permutation is known as its **alternating character**; we express the alternating character of P as $\eta\,(P) = 1$ if P is even and $\eta\,(P) = -1$ if P is odd.

Theorem 2.7. *All permutations are either even or odd.*

Proof. Let P be a given permutation. By theorems 2.1 and 2.3, we know that $P = t_1 t_2 t_3 \dots t_s$, where t_1, t_2, etc. are transpositions. This decomposition is not unique; because $(a\ b)\,(a\ b) = I$, an arbitrary number of products of two equal transpositions can be added to a product of transpositions without changing the value of the product. Furthermore, any transposition $(a\ b) = (c\ a)\,(c\ b)\,(c\ a)$ when c is any object distinct from a and b. Still, the evenness or oddness of P is equal to $(-1)^s$. $\square$

Remark 2.8. It is also clearly a fact that the product of two even or two odd permutations is even, and the product of an odd and an even permutation is odd. Furthermore, $(a\ b)\,(a\ b) = 1$ so the identity permutation is even as well.

3. Constructing the Cube Group

The original Rubik's cube can be described as 26 cubies arranged around a core, which holds the other pieces in place, in the shape of a $3 \cdot 3 \cdot 3$ cube. Each face of the cube is a different color by turning the sides the colored pieces can be mixed up; the goal of the game is to return the pieces to their original configuration. The 26 cubies can be classified as the six center pieces, which have one facelet each, the twelve edge pieces, with two stickers each, and the eight corner pieces, with three stickers each.

Definition 3.1. We will define the sides of the cube as Right, Left, Up, Down, Front, and Back. A **move** X is a ninety-degree clockwise turn of that face. Moves for each face will be denoted as R, L, U, D, F, and B, respectively (we use Up and Down instead of Top and Bottom to avoid the potential confusion between Bottom and Back).

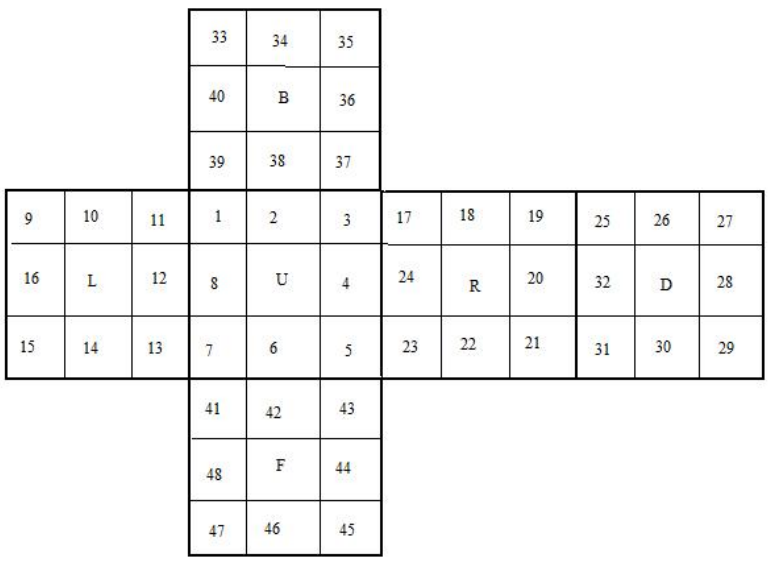

Figure 1. The facelets of the Rubik's cube, numbered in agreement with the set of permutations. If one imagines this diagram folded into the shape of a cube, one can see how each cubie has two or three facelets. For example, the cubie where the Up, Front, and Left faces meet has facelets 7, 41, and 13. Because corner facelets are on the same cubie, they are fixed relative to one another. For example, going clockwise and looking directly at the corner piece, we will never see the facelets in the order 7, 13, 41.

Remark 3.2. Because of the way that the cube rotates, the centers always stay in the same position relative to each other, so we will not consider them. By extension, we will ignore the middle slice turns. For our purposes, a middle slice turn is equivalent to the move XY^{-1} where X and Y are the faces parallel to the middle slice.

With Figure 1, we can explicitly define the effect of each move on the cube. Each of these moves is equivalent to a 4-cycle on the corner cubies of the face in question and a 4-cycle on the edge cubies of the face; considering the moves as two 4-cycles will allow us to look at the possible permutations of cubies without considering orientation later.

$$L = (1\ 41\ 29\ 33)\,(7\ 47\ 27\ 39)\,(8\ 48\ 28\ 40)\,(13\ 15\ 9\ 11)\,(12\ 10\ 14\ 16) \tag{3.3}$$

$$R = (5\ 37\ 25\ 45)\,(3\ 35\ 31\ 43)\,(4\ 36\ 32\ 44)\,(17\ 19\ 21\ 23)\,(24\ 18\ 20\ 22) \tag{3.4}$$

$$F = (7\ 23\ 31\ 15)\,(5\ 21\ 29\ 13)\,(6\ 22\ 30\ 14)\,(41\ 43\ 45\ 47)\,(42\ 44\ 46\ 48) \tag{3.5}$$

$$B = (1\ 9\ 25\ 17)\,(11\ 27\ 19\ 3)\,(2\ 10\ 26\ 18)\,(39\ 33\ 35\ 37)\,(38\ 40\ 34\ 36) \tag{3.6}$$

$$U = (1\ 3\ 5\ 7)\,(2\ 4\ 6\ 8)\,(39\ 17\ 43\ 13)\,(37\ 23\ 41\ 11)\,(12\ 38\ 24\ 42) \tag{3.7}$$

$$D = (19\ 33\ 15\ 45)\,(21\ 35\ 9\ 47)\,(20\ 34\ 16\ 46)\,(25\ 27\ 29\ 31)\,(26\ 28\ 30\ 32) \tag{3.8}$$

Theorem 3.9. *The set of operations on the cube that can be reached from the solved state by making the moves listed above in various combinations is a group under the operation of concatenation. We will then refer to this group as the* ***cube group****.*

Proof.

(1) First we will show that the group has associativity, or that

$$(XY)Z = X(YZ). \tag{3.10}$$

$(XY)Z$ means to do move XY, then move Z, while $X(YZ)$ means to do move X, then move YZ. Both of these are equivalent to making move X, followed by Y, followed by Z.

(2) The identity element, I, is making no move at all. Since this leaves the cube unchanged, we obviously have $IX = X = XI$

(3) The inverse, X^{-1}, of any single face turn is X^3, which is equivalent to the face turn X performed counterclockwise instead of clockwise. The inverse of a sequence of moves XY is $Y^{-1}X^{-1}$. Intuitively, this is clear: the way to undo any sequence of moves is to undo each move in turn, starting with the last move and working back to the first. This can easily be proven by multiplying the two together: $(XY)(Y^{-1}X^{-1}) = X(YY^{-1})X^{-1} = X(I)X^{-1} = XX^{-1} = I$.

□

The cube group is clearly not Abelian: A sequence of two turns acting upon the solved cube, like RU, produces a cube that looks very different from that produced by the sequence UR.

4. Order of the Cube Group

Given what we now know about permutations and the face turns on and structure of the Rubik's cube, we can use combinatorics to calculate the order of the construction group $\mathbf{C}$, or the total number of possible permutations of the cubies.

First, we will solve for the number of possible arrangements of cubies, as if we had taken the cube apart and reconstructed it with the pieces in different places.

The twelve edge pieces may be permuted in 12! ways with 2^12 unique orientations. Similarly, the eight corner pieces can be permuted in 8! ways with 3^8 unique orientations. Thus, there are

$$12! \cdot 2^{12} \cdot 8! \cdot 3^8 = 519,024,039,293,878,272,000 \tag{4.1}$$

possible arrangements of the cubies.

However, not all of these can be reached by our allowed face turns. For example, it is a well known fact among cubers that it is impossible to switch two and only two pieces. This is because each move is the composition of a 4-cycle on the corners and a 4-cycle on the edges. Then each face turn is an even permutation of the cubies. We already showed that the product of two even permutations is even; so only even permutations are possible by means of our allowed face turns. Another way to make the cube unsolvable is to twist a single corner piece or flip a single edge, changing the cube's parity.

For how many of the total permutations do the odd permutations and the permutations with incorrect parity account?

Theorem 4.2. *Exactly half of the permutations in the cube group are even.*

Proof. Let P be an even permutation. Since $PP^{-1} = I$ and I is even, P^{-1} is also even. An even permutation times an even permutation, 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. Now we left-multiply by P^{-1} so that $Q = P^{-1}R$, and the map $Q \longmapsto PQ$ is one-to-one and onto from even to odd permutations. Therefore, either half are even and half are odd, or all are one or the other. In the case of our group, we have examples of both, so half of the total permutations of cubies are even. $\square$

Theorem 4.3. *If one takes out a single corner piece and twists it by $\pm\frac{2k\pi}{3}$ radians, the cube will be impossible to solve. More explicitly: 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 $\frac{2k\pi}{3}$ where k is 0, 1, or 2 mod 3. We will now show that for any permutation of the cube, $k = 0$.*

Proof. Define a map $T : C \to (\mathbf{Z}/3\mathbf{Z})^+$ defined as $T(P) = \frac{3}{2\pi}\sum_{i=1}^{8}\Theta_i = kmod3$ 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 the group $\mathbf{C}$ Now suppose P and Q are elements of $\mathbf{C}$. 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 observation, each of the face turns keeps $k = 0$. Therefore any composition of face turns, and thus any permutation from the solved state, will also have $k = 0$. $\square$

A similar proof holds for a flip of the edge pieces when the rotation is of the form $m\pi$ and m is 0 or 1 mod 2.

Thus, it is impossible to flip a single edge piece, twist a single corner, or switch exactly two pieces. Therefore, half of the permutations will be invalid, as will be half of the edge orientations and two-thirds of the corner orientations. Thus, we have

$$\frac{12! \cdot 2^{12} \cdot 8! \cdot 3^8}{3 \cdot 2 \cdot 2} = 43,252,003,274,489,856,000 \tag{4.4}$$

permutations in the cube group.

5. Diameter of the Cube Group

Currently, it is not known how to find the minimum distance between two permutations of the cube. Current research on the cube group is largely concerned with finding the diameter of the group, or the length of the worst-case shortest solution. The minimum number of turns necessary to solve this worst-case shuffle is known as God's number.

There are two commonly used metrics for counting the number of turns in a given solution. In the quarter-turn metric, each quarter turn counts as a separate move. The face-turn metric is similar except that half turns are also counted as one turn, rather than as two quarter turns. For example, F^2 is counted as one turn in the face-turn metric and two turns in the quarter-turn metric. Solution lengths typically specify which metric is being used by including a q for quarter or an f for face immediately after the number.

A lower bound on God's number can be found with the use of a simple pigeonhole argument that the number of possible positions after n turns must be greater than or equal to the number of permutations of the cube. When the cube is in the initial (solved) state, twelve quarter-turns are possible: one for each of the six faces and their inverses. After that, there are eleven moves that can potentially create a new permutation (twelve, as before, less the inverse of the previous move). Then we have:

$$12 \cdot 11^{n-1} \geq 43,252,003,274,489,856,000 \tag{5.1}$$

where n is an integer. Thus $n \geq 19$ turns in the quarter-turn metric.

The current lower bound, however, is much higher than this. The position known as "superflip," in which all the cubies are permuted correctly with every corner piece oriented correctly and every edge piece oriented incorrectly, was expected for years to require a particularly long minimal solution because of its high degree of symmetry. Furthermore, superflip is unique in that it is the only permutation other than the identity that is in the center of the cube group. In 1995, a 24q solution for superflip was found by University of Central Florida professor Michael Reid, and later proven to be a minimal solution for superflip by Jerry Bryan. Permutations have been found since then that are longer than superflip in the quarter-turn metric. However, superflip has been proven to have a minimal length of 20f, and no positions are currently known that take more than 20 face turns. It's quite possible that superflip's 20f solution is the longest minimal solution for any permutation, and that 20 is God's number in the face turn metric.

However, because of the sheer enormity of the group, proving upper bounds requires an incredible amount of computational power. A new upper bound on God's number, 25f, was published in spring 2008 by Tomas Rokicki. Rokicki's proof makes use of billions cosets to reduce the number of calculations necessary, yet Rokicki still lacked the processing power to make further progress. John Welborn, a representative of Sony Pictures Imageworks, read about Rokicki's proof and was interested enough to offer him downtime on the powerful renderfarm used to create the digital effects used in Sony's films. By June 2008, having used over 55 years of processor time, they had pushed the upper bound down to 24f, then 23f, then 22f. A proof that twenty moves suffice will likely require hundreds of times as much computation as the proof for twenty-two; currently, the limiting factor is only the computational resources available.

Acknowledgments. It is a pleasure to thank my mentors, Vipul Naik and Emily Norton, for their support and guidance this summer. In addition, I'd like to thank Emily Bargar for her inspiration and encouragement. Further thanks go to Stephen Patrias and Ben Schapiro for their unflaggingly generous hospitality.

References

[1] D. Bump. The Mathematics of the Rubik's Cube.
[2] A. Frey and D. Singmaster. Handbook of Cubik Math. Enslow Publishers. 1982.
[3] W. Ledermann. Introduction to Group Theory. Harper and Row Publishers. 1973.
[4] W. Ledermann. The Theory of Finite Groups. Interscience Publishers, Inc. 1949.
[5] J. Palmer. "Cracking the last mystery of the Rubik's cube." New Scientist. 2008.
[6] H. Schwerdtfeger. Introduction to Group Theory. Noordhoff International Publishing. 1976.