Group Theory and the Rubik's Cube

August 19, 2010

Rodrigo Wong*

In mathematics, a group is a topic of great importance. A very important class of groups is the class of permutation groups, since every finite group is isomorphic to a class of permutation groups. Hence, as we will see, the Rubik's cube puzzle can be understood in terms of permutation groups. Therefore, in addition to being a mischievously difficult puzzle, Rubik's cubes provide several tangible examples of groups and of the applications its theory. In this document, we will alternate between a study of group theory and of Rubik's cube, using group theory to find tools to solve the cube and using the cube to illustrate many of the important topics in group theory.

1 Introduction

As Rubik's cube fanatic, it never occurred to me that the structure of the cube was so closely related to group theory. After taking a Modern Algebra course I started to make many connections between the Symmetry Groups and the way that the cube behaved. I started connecting basic terms such as order and closure to the motions of the cube. I then began to wonder if there was a way to solve the cube group-theoretically. After further experimentation and research with the 3x3x3 cube, I found out that many other mathematicians had posed similar questions. Discussing the matter with my advisor, Dr. Sean Lawton, we learned that the 2x2x2 cube, often called the Pocket Cube, was a forgotten yet interesting puzzle to analyze. I began by began by understanding the generators of the permutations group in relationship to the cube. It turned out that the six basic motions of the cube generated the whole permutation group. After consulting with my advisor and discovering that the group generated by these motions was a subgroup of S_{24}, I decided to calculate the size of this group, and found out that the six basic motions generated a group with over 88 million elements. After doing some reasearch on the pocket cube, I discoverd that the game only allowed a total of a little over 3 million allowed configurations. It was then when I recalled that Joseph Gallian mentioned in, Contemporary Abstract Algebra, that cubes possesed a group of rotations. Because of this, I discovered that many of the elements on the group generated by the basic motions, exactly $\frac{1}{24}$ of them, were equivalent through rorations. After finding out the order of ther allowed color configurations, it remained to show a group theoretical way to reach a solution to this puzzle. Through further experimentation with the cube, I realized that in most cases, the last layer of the cube could be solved by permuting three corners. Could it be that after eliminating the group of rorations, the whole cube could be solve in the same fashion?

2 Permutation Puzzles

A permutation puzzle is a one person game with the five properties listed below. Before listing the properties, we define puzzle position to be an element in the set of all possible legal moves. The five properties of a permutation puzzle are :

1. For some $n > 1$ depending only on the puzzle's construction, each move of the puzzle corresponds to a unique permutation of the numbers in $T = 1, 2, ..., n$,

2. If the permutation of T in (1) corresponds to more than one puzzle move then the the two positions reached by those two respective moves must be indistinguishable,

3. Each move, say M, must be "invertible" in the sense that there must exist another move, say M^{-1}, which restores the puzzle to the position it was at before M was performed,

4. If M_1 is a move corresponding to a permutation f_1 of T and if M_2 is a move corresponding to a permutationf_2 of T then $M_1 * M_2$ is either not a legal move, or corresponds to the permutation $f_1 * f_2$. Recalll that for permutations the group operations * means functions compositions and for moves * means performing two moves in sequence.

3 Group Theoretic Description of the 2x2x2 Cube

As a permutation puzzle , it is important to define the rules under which the Cube works. There are three cardinal directions, fixing an orientation of the cube in space with respect to one of this directions and there are two directions in which the cube can be rotated. We refer to these motions as a 90 degree rotation clockwise or counterclockwise depending on the direction of the rotation. Note that since rotations are made on 90 degree intervals, after turning a face four times, we will return to its original place. These six moves (three orientations in space with two rotations each), along with any combination of them, make up the basic motions that are allowed in the game. What we mean by this is that any possible configuration on an scrambled cube, can be obtained by using a combination for each face rotation.

There are four stickers on each face and a total 24 stickers. The set of permutations of all 24 stickers is equivalent to the group of symmetry S_{24}. However, not all sticker configurations constitute a valid or allowed color combination that can be reached by the allowed moves. In order to make more sense of the motions previously mentioned, we will use the diagram below in order to properly define the notation used when referring to the legal motions of the game.

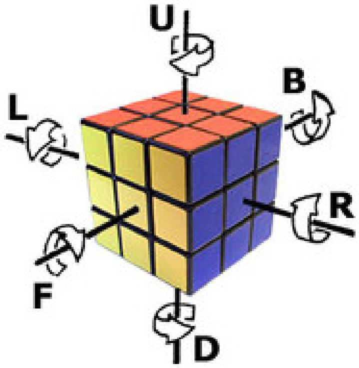

Fig. 1 Rubik's Cube Notation (source: http://rubiks.wikia.com/)

Each face of the cube us assigned a letter: F,R,U, D, L, and B, corresponding to front, right, up, down, left, and back, respectively. They are oriented with each other as is demostrated in figure 1. These letters also correspond the the 90 degree clock-wise and couunter-clock-wise ;that is, corresponding to clock-wise 90 degree rotations around the normal vector of each respective face. motions descriebd earlier. For example, F denotes the move that rotates the front face, f, by 90 degrees clockwise. Similarly, using the same notation, we are able to denote the inverse of a motion. For example, we express a 90 degree counterclockwise rotation of the front face with F^{-1}.

Remark 1. Function composition would suggest that FR implies a turn on the Right face followed by a turn on the Front face. However, convention in Rubik's cube language dictates that FR means a turn on the Front face followed by a turn on the Right. (When it comes to cube algorithms, it is a lot more natural to perform the motions as you see them than having to translate them into function composition notation).

The figure below shows a two-dimendional diagram of the cube. Looking at the cube in this way allows us to understand how the motions permute each sticker. Note that the number in the labeling shows us how a given motions permutes the stickers on the cube. Once the notation has been fixed, there is only one way a particular motion. With that said, all permutations mentioned below will be written with respect to figure 2.

```
                +---------+
                | 1     2 |
                |    u    |
                | 3     4 |
      +---------+---------+---------+---------+
      | 13   14 | 5     6 | 17   18 | 21   22 |
      |    l    |    f    |    r    |    b    |
      | 15   16 | 7     8 | 19   20 | 23   24 |
      +---------+---------+---------+---------+
                | 21   22 |
                |    d    |
                | 23   24 |
                +---------+
```

Fig. 2 Unfolded Labeled Cube

Definition. The symmetry group on 24 stickers is the set of bijections from {1,2,...,24} to {1,2,...,24}, with the operation of function composition. We write this group as S_{24}.

Starting with the solved cube, let numbers on each face represent the four stickers of the cube. When a given face turn is performed, all stickers affected by that motion are permuted to a new position in the cube. Below are the permutations originated from each motion with respect to Figure 2. Recall that all allowed position of the cube can be obtained by performing a combination of the following motions.

U= (5 13 21 17) (6 14 22 18) (1 2 4 3)
R= (6 2 23 10) (8 4 21 12) (17 18 20 19)
F= (5 6 7 8) (3 17 10 16) (14 4 19 9)
D= (7 19 23 15) (8 20 24 16) (9 10 11 12)
L= (13 14 16 15) (5 9 24 1) (7 11 22 3)
B= (21 22 24 23) (2 13 11 20) (1 1512 18)

It is good to point out that a sequence of movements such as FF can be expressed as F^2. Similarly, FFF is often expressed as F^3, $LFLFLFLF$ as $(LF)^4$, and so on.

Now that the notation has been established, I find it of importance to justify that the cube does in fact satisfy the properties of a group. Recall that there are four properties that a set must satisfy in order to be a group. The set must be closed under the group operation, it must have an identity, all elements must have an inverse, and the operation must be associative. In the case of the 2x2x2 cube, the operation is the rotation of a face by 90 degrees. The group of elements themselves are sequences of moves, which are the set of all admissible permutations or configurations of the cube.

1. Closure is present, since performing any two operations still yields an admissible configuration of the cube.

2. There is an identity: the move in which no rotations are performed to the cube.
3. Every element has an inverse, becaues a face can be rotated either clockwise or counterclockwise.
4. The operation is equivalent to function composition, thus it is associative.

Another direct consequence of our notation showsto that $F * F^3 = F^4 = e$. Thus, we can conclude that $F^3{=}F^{-1}$. Consider F^4; this is the first time that performing$F$ repeatedly takes us to the solved cube, e. The motions F,R,U, D, L, and B all have order 4. However, the sequence of moves $S{=}L^2F^2$ has order 12 and the sequence of moves $T{=}LF$ has order 28 (try it out!).

4 Full Group of Motions

We established on the previous section that six basics motions generate all the possible sticker configurations that are legal in regards to the Rubik's cube game. It now remains to find out exactly how many legal sticker configurations these motions generate. By using GAP, a computational algebra software package, I discovered that these six elements generated a group with 88,179,840 elements. Each element of the group generated corresponds to a combination of these six generators.

Proposition. *The group of basic motions $G{=}< U, F, R, L,D, B>$ generates the group of all possible allowed configurations C.*

Proof. Because every element in C can be obtained as a combination of motions in G and since all motions in G are reversible, we can conclude that the six basic motions generate C. □

As I analyzed the complete group of motions of the cube, it occured to me that there was a subgroup of motions that I was not taking into account. The cube can be rotated in space, and by doing so, we permute the stickers to a rotational equivalence of the identity. This led me to the realization that consistency on my orientation was essential. Once a face is chosen as the front all configurations of the cube must be realized with the same orientation. With this in mind, and with a little help from Joseph Gallian's Contemporary Abstract Algebra, I found the group generated by the rotations of the cube:

α= (5 7 8 6) (21 22 24 23) (13 11 20 2) (15 12 18 1) (15 12 18 1) (14 9 19 4) (16 10 17 3)

β= (13 14 16 15) (20 18 17 19) (11 22 3 7) (9 24 1 5) (12 21 4 8) (10 23 2 6)

I used GAP to calculate the order of $R{=}{<}\alpha, \beta{>}$ and found that it was 24. This led me to another question: what relevance does the order of R have with respect to C? Through physical experimentation with the cube, I found out that the group of rotations creates repeating configurations with respect to the group generated by the six allowed motions. This means that $\frac{1}{24}$ of the number of elements of G=$<U, F, R, L,D, B>$ are rotational equivalences. This equivalences are defined and studied in more detail in the next section.

5 Color Admissible Positions

Definition. Color Admissible Positions.

Consider the group of all allowed configurations of the cube C and the group of rotations of the cube R. We know that group of motions C is a subgroup of of S_{24} ;thus, every element in C corresponds to:

a. An allowed sequence of motions (in terms of F,R,U, D, L, and B) starting from the solved cube.

b. An allowed position of the colors of a cube. We refer to this positions as the simplified elements of M in S_n.

The admissible positons are the allowed are the simplified (in S_n) elements of C. In relationship to the cube, these are the allowed sticker configurations.

The color admissible configurations, as defined above, are the possible combinations that the rules of the game allows the cube to have. That is, any combination of color stickers that a solve cube has after performing the basinc motions or any combination of those motions.

Because we are rearranging the stickers on the cube, it is more convenient to leave the cube as a game and venture in the the world of permutation groups. Recall the following definitions:

Definition. If R is a subgroup of C (though R can be C), then R can act on the set C by left multiplication. Any r in$R$ acts on c in C to give rc in C, that is C/R= $\{Rc \mid c \in C\}$

The **orbits** of this action are sets of the form Rc, are called left cosets. If needed, we could have used multiplication from the right, to give the orbits cR which are called right cosets.

The orbit of an element R is the set containing rc for all c in C .

Claim. $Orb_R(c)$=$\{rc \mid c \in R\} \forall c \in C$, $|Orb_R(c) \mid = \mid R \mid$

Proof. It follows from Lagrange's theorem that $|C/R \mid = \mid C \mid / |R|$. Then,

rc_1= $r^{'}c_2 \subset Rc_1$

c_1= $(r^{-1}r^{'})c_2$

and thus,

$Rc_1 = Rc_2$ □

6 Color Equivalent Motions

As mentioned above, the group of rotations on the cube creates color equivalence positions with respect to the group of total configurations of the cube C. The following defiftion is relevant to the game because it provides us with the final ingredient needed to provide a good description of the allowed positions that are relevant to the game.

Definition. Color Equivalent Motions

The allowed color configurations or admissible possitions are color equivalent if and only if the are related by a 3 dimensional rotation.

Recall that $|C| = 88, 179, 840$ and that $\mid R \mid = 24$. In the previous section, we learned that the group of rotations created color equivalences with respect to C. Thus, by eliminating these rotational equivalences and by the definition of color equivalence, we find the the number of unique color arrangements of the cube is 3,674,160. The reason is that the 3,674,160 figure implicitly assumes that cubes that differ only in orientation of the overall cube are equivalent, and there are twenty-four ways to orient the cube in space (i.e., the order of the rotation group of the cube is 24).

Though it remains to be proved, my intuition and expertise with the cube suggest that the equivalence classes on the 2x2x2 cube are generated by the two rotational symmetry groups and one group of reflectional symmetry. I believe that most equivelence classes have 24*24*2= 1152 elements, although some may have fewer.

Now that we have defined the color equivalent motions of the cube, it follows that by the eliminating the rotational equivalences we can describe the cube in termns on only three generators. In GAP I calculated the size of a group generated by onle three of the six basic motions indeed, the order was the same as C/R.

Claim. Let $C_1 = < U, F, R, \alpha, \beta >$ then, $MR = C$ where $M = < U, F, R >$

Proof. Let ϕ: $M \times R \rightarrow C$

then, $(m, r) \rightarrow (mr)$

Since $M \cap R = \{ e \}$, then

$m_1 r_1 = m_2 r_2$

$m_2^{-1} m_1 = r_2 r_1^{-1}$

but $m_2^{-1} m_1 \in M \cap R = \{ e \}$

then $m_2^{-1} m_1 = e$ and so $m_1 = m_2$

And thus ϕ is one-to-one.

It now remains to show that ϕ is onto. By assumption, $MR = C$, thus

$\mid \phi (M \times R) \mid = \mid M \times R \mid = \mid C \mid$ and so ϕ is onto. □

Proposition. *For all $x \in M$ there exist a unique $Rc \in C/R$.*

Proof. We first proceed to find the existence of such element.

Let $x \in M \subset C$, then Rx is an element of C/R.

We now show uniqueness:

Assume $Rx = Ry$ then,

$rx = r^{'} y \implies r(r^{'})^{-1} \in M \cap R = \{ e \} \implies r = r^{'}$ and so $x = y$. □

7 Solving the Cube

Before we can dive into the group theoretic approach to solve the cube, let us recall the following definitions.

Definition. Group Action

If G is a group and X is a set, then a (left) group action of G on X is a binary function

$G \times X \to X$ denoted denoted

$(g, x) \mapsto g \cdot x$

which satisfies the following two axioms:

1. $(gh)\cdot x = g\cdot(h \cdot x)$ for all g, h in G and x in X;

2. $e \cdot x = x$ for every x in X (where e denotes the identity element of$G$).

The set X is called a (left) G-set. The group G is said to act on X (on the left).

An action is transitive if for any two elements a and b in the set A, there is some g in G such that ag=b. This means that the orbit of any element is the whole set, so aG=A for any a in A.

Definition. Commutator

If g and h are elements of the group G, then the commutator of g and h is the element $g^{-1}h^{-1}gh$. The commutator is a measure of how much the elements g and h commute, if they do commute then the commutator is the identity. The commutator of g and h is sometimes denoted by $[x, y]$.

Remark. The commutator subgroup of G is the subgroup generated by all commutators in G. Note that the commutator group is not just the set of commutators itself but is generated by that set, as this set is not necessarily closed and therefore is not necessarily a group in its own right.

Commutators are a source of useful move sequences. Since a commutator is a measure of how near two elements commute, taking a commutator of two elements that nearly commute will give something that moves very little and hence is likely to have a useful effect. The next theorem

Theorem. *Half of the allowed sticker configurations of the cube can be solved with just commutators the other half can be solved by commutaros and a sequence of moves of order two.*

Proof. Given a color equivalent position Rc (any given possibility of a mixed up cube) there exists an element $p \in Rc$ so that $p \in M$.

There also exist elements $s \in [\ M\ ,\ M\ ]$ and $z \in \mathbb{Z}_2$ so $(\ sz\ )\ p = e$ [since M acts transitively on itself. □

GAP Codes

Group generated by 6 basic motions

```
    U:=(5,13,21,17)(6,14,22,18)(1,2,4,3);
    R:=(6,2,23,10)(8,4,21,12)(17,18,20,19);
    F:=(5,6,8,7)(3,17,10,16)(14,4,19,9);
    D:=(7,19,23,15)(8,20,24,16)(9,10,12,11);
    L:=(13,14,16,15)(5,9,24,1)(7,11,22,3);
    B:=(21,22,24,23)(2,13,11,20)(1,15,12,18);
    C:=Group(c1,c2,c3,c4,c5,c6);
    Group generated by rotations
    r1:=(5,7,8,6)(21,22,24,23)(13,11,20,2)(15,12,18,1)(14,9,19,4)(16,10,17,3);
    r2:=(13,14,16,15)(20,18,17,19)(11,22,3,7)(9,24,1,5)(12,21,4,8)(10,23,2,6);
    R:=Group(r1,r2);
    Group of color equivalences
    M:=Group(c1,c2,c3);
    Commutator subgroup
    L:=CommutatorSubgroup(M,M);
    GeneratorsOfGroup(L);
    l1:=(2,23,21,12,18,20)(3,4,14,6,5,17);
    l2:=(1,3,22,14,13,5)(4,19,17,10,6,8);
    l3:=(2,6,18,17,21,4)(7,19,9,10,16,8);
    l4:=(1,3,22,14,13,5)(4,23,17,12,6,20)
```

References

[1] David Joyner, Adventures in Group Theory, Johns Hopkins University Press, 2002.

[2] Joseph Gallian, Contemporary Abstract Algebra, Houghton Mifflin College Div; 4th edition, 1998.

[3] GAP User's Manual - http://www-gap.mcs.st-and.ac.uk

[4] Dr. Sean Lawton, Assistant Professor - The University of Texas PanAmerican.