The Permutation Group of the Rubik's Cube

Lucas Garron

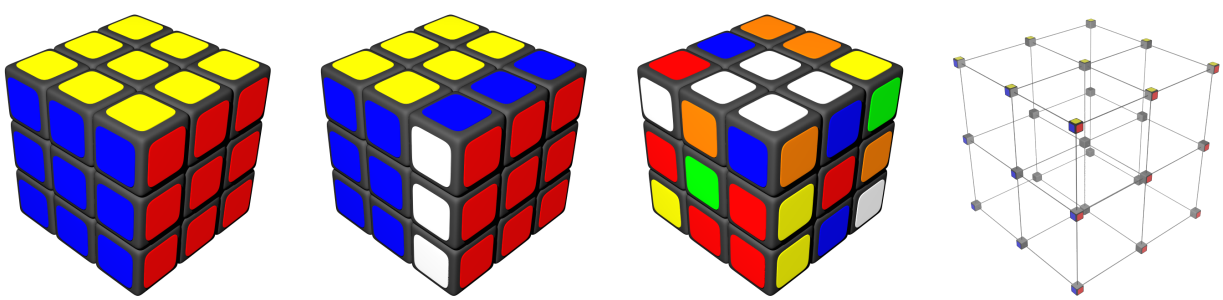
March 8, 2010

1 Introduction and Motivation

The **Rubik's Cube** (Figure 1a) is a widely known cultural icon. It is a mechanical puzzle which can be visualized as a three-dimensional 3x3x3 array of 27 unique **cubies**, where the visible outer faces of the cubies are covered with **stickers** colored according to their orientation. From this **solved** state, any outer "slice" of 9 cubies may be rotated to permute the cubies –Figure 1b shows the effect of such a **turn**. The objective of the puzzle is to return it to its solved state after any arbitrary move sequence has been performed on it. Since any cubie is uniquely defined by the arrangement of colors on it, the task amounts to restoring each cubie to its original configuration.

The Rubik's cube exhibits a **group structure**, which makes it a great tool for understanding group theory –and vice-versa. Its structure and non-trivial complexity (size) amenable to advanced mathematical and computational analysis. Although several fundamental questions in Rubik's Cube theory are unresolved (the diameter of its Cayley graph is unknown), there are various established topics. This paper aims to be an exposition to the question "What are the conjugacy classes of the cube?"

Aside from the curiosity, part of the motivation stems from the author's practical interest in speedcubing. **Speedcubing** is the sport of solving a Rubik's Cube as fast as possible, in various ways. The specific category of **blindfolded solving** involves memorizing a cube and then solving it without looking at it. This is commonly done by using a cycle decomposition of the state, and is a practical situation where theoretical understanding of the structure of the cube is a great asset.



(a) A Rubik's Cube in its unique solved state.

(b) A solved Rubik's Cube after one move performed on its right side: R.

(c) An arbitrary arrangement of the cube, reached by performing successive turns.

(d) A exploded view of the cubie arrangement structure.

Figure 1: The Rubik's Cube

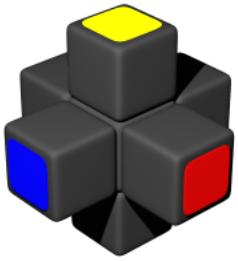
2 The Rubik's Cube as a Group

2.1 Definitions

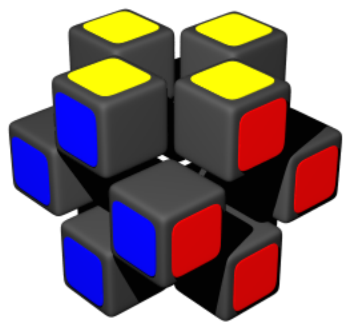
There are 4 types of cubies comprising our abstraction of a Rubik's Cube:

- 1 fixed **core** with 0 stickers. (Figure 2a)
- 6 fixed **centers** with 1 sticker each. (Figure 2a)
- 12 **edges** with 2 stickers each, and 2 valid orientations for each position. (Figure 2b)
- 8 **corners** with 3 stickers each, and 3 valid orientations for each position. (Figure 2c)

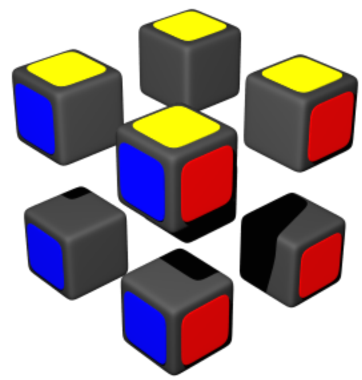
Each cubie faces outward on a different set of faces, so cubies of the same type can be distinguished by their sticker colors.



(a) The **frame** of a Rubik's Cube: a **core** surrounded by 6 center cubies.



(b) The 12 **edge** cubies.



(c) The 8 **corner** cubies.

Figure 2: Types of cubies comprising a Rubik's Cube

Definition 1. **E** *is the set of permutations of the 12 edges along with their orientations, comprised of a permutation* **EP** *of edges along with a set of orientations* **EO** *for the 12 locations of edges. Similarly, we define* **C**, **CP**, *and* **CO** *for the 8 corners.* [1]

Definition 2. *A* **state** *of the Rubik's Cube is a physically realizable arrangement of cubies. Since the core and centers do not move from their places, every state is be represented by an arrangement of cubies $\in E \times C$ (Cartesian product).*

Definition 3. *Let* **qturns** $= \{B, F, U, D, L, R\}$ *correspond to the* $\{back, front, up, down, left, right\}$ *sides of a cube, respectively. Each letter denotes the operation of rotating the 9 cubies sharing a sticker on the relevant side, clockwise when viewed facing that side. (Figure 1b shows an R-turn in perspective.) For all $t \in$* **qturns**, *we also define $t2 = t^2$ and $t' = t^{-1} = t^3$ for brevity, and* **hturns** $= \{B, F, U, D, L, R, B2, F2, U2, D2, L2, R2, B', F', U', D', L', R'\}$. [2]

[1]Under composition, $EP \cong S_{12}$, $EO \cong \mathbb{Z}_2^{12}$, and E is their **semi-direct product** $EO \rtimes EP$ (and $CP \cong S_8$, $CO \cong \mathbb{Z}_3^8$, $C = CO \rtimes CP$). However, we will focus on EP and CP, so this structure is not as relevant to us.

[2]Note that cube moves are traditionally composed in left-to-right order. For examuple $R'\ U2 = RRRUU$ is a move sequence (a **word** in group theory) representing the compound operation of performing R', then $U2$.

Also, edge and corner cubies are named by the sticker faces corresponding to its solved location. For example, the *yellow-blue* edge in Figure 1b is called UF, and the *white-blue-red* corner is called DFR.

Definition 4. *A* **valid state** *of the Rubik's Cube be a state of the cube that can be reached by performing a sequence of* **qturns** *on the solved state.*

2.2 Group Theory

As advertised, the Rubik's Cube can be represented as a group.

Definition 5. *Let* **T** *denote the set of permutations 54 stickers on the cube, so that* $S_T \cong S_{54}$ *is a group.*

Since all the cubies can be identified by their stickers, each valid state of the group corresponds to an element of T.

Theorem 1. *The valid states of the Rubik's Cube comprise a group* $\mathbf{G}$.

Proof. The valid states are the elements of T generated by compositions of the sticker permutations of *qturns*. Thus, G is isomorphic to the subgroup of $S_T \cong S_{48}$ generated by $\langle qturns \rangle = \langle \{B, F, U, D, L, R\} \rangle$ □

The identity element of G is the solved state, and the other properties of a group are conveniently inherited from generating it as a subgroup.

Let $G' = E \times C$ (a direct product of edge and corner states). G' is sometimes called the **screwdriver group**, because it corresponds to set of the states that can be reached by prying the cube apart with a screwdriver and assembling it arbitrarily. The following theorem should be obvious:

Theorem 2. $G \subseteq G'$.

Proof. G is the set of valid states, and G' is the set of all states (Definition 2 interpreted group-theoretically), so $G \subseteq G'$. Therefore, the valid states of the cube are a subgroup of the arrangements of the pieces. □

In fact, G is a proper subgroup of G', with index 12. We will not prove this, but this arises from the following:

Theorem 3. *The group action of G on EO has index 2 in EO,*
the group action of G on CO has index 3 in CO,
the group action of G on $EP \times CP$ has index 2 in $EP \times CP$, and
G has index 12 in $G' = (EO \rtimes EP) \times (CO \rtimes CP)$ [1]

Corollary 1 (Size of the cube group / number of valid states)**.**

$$|G| = \frac{|G'|}{12} = \frac{|EO| \cdot |EP| \cdot |CO| \cdot |CP|}{12} = \frac{2^{12}\ 12!\ 3^8\ 8!}{12} = 43,252,003,274,489,856,000$$

We have been playing a little loose with notation, and have not actually explained the semi-direct product in the expression above.[3] However, we will give an idea of the arguments using a related group, the cubie permutation group (ignoring orientation).

[3]It arises from the fact that the in-place cubie orientations are a normal subgroup of the cube: orienting in place is still equivalent to orienting in place after conjugation.

2.3 The Cubie Permutation Group

What happens if we ignore orientation, and only care about the location of each cubie? (Suppose each cubie were assigned a single identifying number instead of three stickers, and the solved state only needed each number in place).

Definition 6. *Let $P' = EP \times CP \cong S_{12} \times S_8$. The cubie permutation group P is the group action of G on P'.*

P' might be called the **cubie permutation screwdriver group**. Any permutation of edges is possible, and any permutation of corners is possible. However, in P', they are subject to joint parity. We will lead up to this formally.

Theorem 4. *G is 12-transitive on EP.*

Proof. We seek to generate any edge permutation. We split this into odd and even permutations:

- Suppose a is an even permutation in $EP = S_{12}$; that is, $a \in A_{12}$. Since the 3-cycles generate A_{12} ([2], pg. 30), it suffices to show that we can generate any 3-cycle. This is possible:

  Proof. $R'LF2RL'U2$ is the net permutation $(UB\ \ UF\ \ DF)$ in E. It is not hard to see that any three edges can be brought to these locations to perform an arbitrary 3-cycle. [4] □

- Suppose a is an odd permutation in EP. Since applying a single R-turn is an odd permutation (four-cycle) on edges, $a' = aR$ (state a composed with an R-turn) is even, and we can generate a by generating $a = R'a'$

□

Therefore, any permutation of the 12 edges is possible, and by a very similar argument, any permutation of the 8 corners is possible:

Theorem 5. *G is 8-transitive on CP.*

However, G does not act transitively on P'.

Theorem 6. *(a, b) $(\in EP \times CP)$ is in P' precisely when the parity of permutations a and b match. This is often called the* **permutation parity restriction***.*

Proof.
- Proof of the forward direction:
  Any (a, b) in P is generated by $\langle turns \rangle$, starting from (e, e) (which is $(even, even)$ parity). Each turn $\in qturns$ performs a 4-cycle of edges and a 4-cycle of corners, changing the parity of both symmetric groups in tandem. Any (a, b) is thus finitely generated with matching parity.

[4]Intuitively, the induced subgroups of E remain transitive after we restrict our generators to stabilize UB ($\{F, D, L, R\}$) after permuting an arbitrary edge there, and again for UF ($\{D, L, R\}$). Essentially, there is a lot of room on the cube to maneuver three edges.

- Proof of the converse direction:
  By theorem 5, we can generate (a', b) for some a' matching the parity of a. By using the same procedure as the proof of theorem 4 (since the cycle used in the proof does not affect corners), we can also generate (a, b) (although we would use b to get into the odd coset of A_{12}).

□

Thus, the permutation parity of edges and corners are tethered to each other, but otherwise, the permutations are free. Therefore, the index of P in P' is 2: $|P'| = |EP||P'/EP| = |12!||8!/2| = |P|/2$.

2.4 Conjugacy classes of P

Let us move on to conjugacy classes, which describe the fundamental different ways that cubies can be permuted with each other.
Recall the fact that a group H may be partitioned into conjugacy classes, disjoint subsets where each pair of elements a and b in a the same set are conjugate to each other ($\exists c \in H$ such that $a = cbc^{-1}$).
Let us state a basic observation about conjugacy classes:

Theorem 7. *The conjugacy classes of S_n correspond to the $p(n)$ unordered integer partitions of n, where the partition of n lists the lengths of the cycles of the permutation.*

For example, $\{4, 3, 3, 2\}$ is a partition of 12, corresponding to the conjugacy class of permutations of S_{12} with a 4-cycle, two 2-cycles, and a 2-cycle (e.g. $\{2, 3, 4, 1, 6, 7, 5, 9, 10, 8, 12, 11\}$).

We can compute that EP has $p(12) = 77$ conjugacy classes, and CP has $p(8) = 22$.

Definition 7. *Let G be a group. $C(G)$ will denote the set of conjugacy classes of G.*

Theorem 8. *Let $G = A \times B$. Then $C(G) = C(A) \times C(B)$*

Proof. Let $\alpha \in C(A), \beta \in C(B)$ be any conjugacy classes, and $a \in \alpha, b \in \beta$. Then $(a, b) \in G$ can only be conjugate to another element $(c, d) \in G$ if both components are conjugate: $c \in \alpha, d \in \beta$. Thus, the conjugacy classes of G are all combinations (α, β) in $C(A) \times C(B)$. □

Corollary 2. *$P' = EP \times CP$ has $1694 = |C(P')| = |C(A) \times C(B)| = 77 \cdot 22$ conjugacy classes.*

But what are the conjugacy classes of P?
We can say that a conjugacy class is even if its members are all even permutations (there are an even number of cycles of even length), and complementarily for an odd conjugacy class.

By enumerating the conjugacy classes and counting (say, using a computer), we find that

- EP has 40 even and 37 odd conjugacy classes, and
- CP has 12 even and 10 odd conjugacy classes.

Theorem 9. *P has $40 \cdot 12 + 37 \cdot 10 = 850$*

Proof. The conjugacy classes of P are the conjugacy classes of P' that satisfy the parity constraints. Thus, it is the union of the direct products of the even conjugacy classes, and of the odd conjugacy classes, of cardinality $40 \cdot 12 + 37 \cdot 10 = 850$. (All the permutations corresponding to these classes do exist in G.) □

2.5 P vs. G

The enumeration of conjugacy classes of the entire group G is significantly more complex, with subtle details. It is easiest to approach the same way as above, but with net "twists" denoting the total orientation of each cycle.
In addition, several even permutations with the same cycle structure are not conjugate, due to the following "false theorem." (Jerry Bryan, [3])

False Theorem 1. *If $x, y \in G$ have the same cycle structure, they are conjugate.*

This is true if G is a symmetric group S_n, and the converse *is* a theorem. However, there are valid cube states in G with the same cycle structure of stickers, but who cannot be conjugated to each other.[5]

Furthurmore, there are certain parity-sensitive permutations which fall into different conjugacy classes depending on the permutation used to conjugate them.

The total number of conjugacy classes is now the sum of products for even, odd, and parity-sensitive classes:

$$308 \cdot 140 + 291 \cdot 130 + 17 \cdot 10 = 81120$$

3 Conclusion

Extending the main goal of this paper, the question of conjugacy classes is surprisingly rich, because the details are very subtle. The author himself barely understands the reason for some of the calculations, and wonders why this problem is not well-documented in cube theory literature. It is still possible to extend the analysis to other puzzles and groups, and even for the $3x3x3$ Rubik's Cube, it it is still possible to refine the counts into explicit lists, and a full data set of the sizes and orders of the conjugacy classes would allow interesting analysis that allows us to explain some of the general behavior of all the valid states in new ways. (This information is apparently not accessible to the speedcubing community yet.)
In addition, there are many basic results in cube theory, which are surprisingly accessible with basic knowledge.[6] Basic and advanced concepts in cube and group theory are also often easier to understand together, and the hope is that this paper will expose some future group theorists to a little peek into the technical world of the cube.

References

[1] David Joyner. *Adventures in Group Theory.* John Hopkins University Press, 2nd edition, 2008.

[2] M. A. Armstrong. *Groups and Symmetry.* Springer, 1988.

[3] Jerry Bryan et al. Conjugacy classes of the cube. Online Discussion, http://cubezzz.homelinux.org/drupal/?q=node/view/161, October 2009.

[5] For example, $U2B2R2D2U2R2F2U2$ and $B2R2U'B2L2BFRB2RB'FD'F2D2R2$ are both comprised of 12 2-cycles of stickers, but are not conjugate.

[6] Tomas Rokicki, a prominent computer cubing expert, remarks that there is a lot of "low-hanging fruit" in the subject that has yet to be investigated.