Introduction of Several Special Groups and Their Applications to Rubik's Cube

Yutong Gu

Broward College, Hangzhou, China

guy5@mail.broward.edu

Abstract. Group theory is the subject that aims to study the symmetries and structures of groups in mathematics. This work provides an introduction to group theory and explores some potential applications of group theory on complex geometric objects like the Rubik's cube. To this end, the concepts of symmetric group, permutation group, and cyclic group are introduced, and the famous Lagrange's theorem and Cayley's theorem are mentioned briefly. The former theorem establishes that a subgroup's order must be a divisor of the parent group's order. Concerning the permutation group, it is a set of permutations that form a group under composition. Hence, the various groups that can be formed by the Rubik's cube are discussed, including the group of all possible permutations of the cube's stickers, and the subgroups that are generated through permutations of the six basic movements embedded in Rubik's cube. Overall, this essay provides an accessible introduction to group theory and its applications to the popular Rubik's cube.

Keywords: Group theory, Permutation group, Cayley's theorem, Rubik's cube.

1. Introduction

Hitherto, group theory is a fundamental and important area of mathematics that has a wide range of applications in many different research fields, including physics, chemistry, computer science, and cryptography. It is a versatile and powerful tool for understanding symmetry and algebra [1]. There are many useful groups and theorems in group theory, and the present work serves as an introduction to several basic topics in group theory. It commences by defining the symmetric group, which is a group over all the sets with elements that are consisting of every bijection operation. It then defines the permutation group, which is the set of all bijections and satisfies the law of composition. Additionally, the essay also introduces the cyclic group, which is a subgroup that belongs to a parent group formed with one generator. In addition, the essay provides an explanation and a brief proof of Lagrange theorem and Cayley's theorem, which are both fundamental theorems about algebraic structures and have far-reaching impacts on many research areas.

Apart from these basic topics, this work also explores the potential applications of group theory on Rubik's cube [2]. A permutation group is a subset of bijection operations from group G. Here, all the elements in that group are permutations of group G, and the composition of permutations in group G is group operation. Permutation groups are often used to study the permutations of different status of objects. In this paper, in order to study the of Rubik's cubes from the perspective of group theory, variations of Rubik's cubes are transformed into the form of permutation groups. In doing so, one can simulate them by some permutation groups. Interestingly, the results indicate that the variations of Rubik's cubes can be simulated by some permutation groups, and these variations can be considered as subgroups of the permutation group S_{54} as there are 54 blocks in total. This finding highlights the versatility of group theory and its power in exploring and understanding complex systems in various research fields.

2. Special Groups and Relevant Theorems

2.1. Symmetric Group

The symmetric group is the group over all the sets with elements that are consisting of all bijection operations. Its group operation is the combination of its functions [3]. For a symmetric group of order

n, it acts on a set $X = \{1, 2, 3, \dots, n\}$. As a typical example, the symmetric three-order group $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ is such a group that acts on the set $X = \{1, 2, 3\}$.

2.2. Permutation Group

A permutation is a way to arrange objects in a specific order or sequence. A permutation group is a mathematical group consisting of bijective mappings (permutations) from a set to itself. In other words, it is a collection of permutations of a given set that satisfy certain algebraic properties [4]. Specifically, a permutation group must be closed under composition, and should contain the identity and the inverse. It is a bijective function that maps a set to itself so as to each element appears only one time in the resulting arrangement.

Let X be a set. The set of all bijections of X satisfies the condition that $P(x) = \{f: X \to X | f \text{ is bijective}\}$ and they form a group. The targeted group is named as the permutation group on X. When X is a set of n elements, it is useful to rename the elements by the numbers $1, 2, \cdots, n$, and call it as permutation group of n (denoted by S_n). For example, $\sigma = \binom{1\,2\,3\,4}{2\,3\,1\,4}$ is a permutation group for the set $G = \{1, 2, 3, 4\}$ with permutation $\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1$ and $\sigma(4) = 4$. Suppose that X is a permutation group, then it satisfies the following conditions which contain that the associativity property holds for the composition of functions, the identity element is represented by the identity function on X: $\forall f \in P(X), f \circ idX = idX \circ f = f$, and the inversion of $f \in P(x)$ is its inverse function f^{-1}: $f \circ f^{-1} = f^{-1} \circ f = idX$.

2.3. Cyclic Group

Suppose that G is a group while x belongs to G. The cyclic subgroup of G is created by x and it is a special set that owns all powers of x: $\langle x \rangle = \{x^k \in G | k \in Z\}$. If $|\langle x \rangle|$ is infinite, then it is said that x has infinite order. If $|\langle x \rangle|$ is finite, one can define the order element x as $|x| = |\langle x \rangle|$, i.e., the order of cyclic subgroup is generated by element x [5]. Further, if $x \in G$ and $G = |\langle x \rangle|$, then group G is a cyclic group and x is regarded as the generator of that group.

Let $\sigma = \binom{1\,2\,3\,4}{2\,3\,1\,4}$ be a cyclic group for the set $G = \{1, 2, 3, 4\}$. Since $1 \to 2,\ 2 \to 3,\ 3 \to 1$, then $(1\ 2\ 3)$ is a cycle of the cyclic group. Similarly, (4) is another cycle of the cyclic group. Hence, $\sigma = \binom{1\,2\,3\,4}{2\,3\,1\,4}$ can also be written in cycle notation $(1\ 2\ 3)(4)$.

2.4. Lagrange's Theorem and Cayley's Theorem

Within the context of group theory, Lagrange's theorem establishes that the degree of a subgroup H should be the factor of the corresponding finite group G. In other words, if H is the subgroup of a finite group G, it is satisfied that $|G| = [G: H] * |H|$ [6]. To be clear, $|G|$ denotes the degree of the group G, which is exactly the number of elements in G. Similarly, $|H|$ stands for the degree of the subgroup H, and $[G: H]$ denotes the index of H in G. Lagrange's theorem is a fundamental result in group theory that relates a subgroup's order to the order of the large group.

Cayley's theorem establishes that each group G is isomorphic to a subgroup of symmetric group S_n. It is considered as group G acts on its elements. In other words, a group G could always be represented by a group of permutations on its own elements [7]. Specifically, for any group G, there exists a subgroup of a given symmetric group G. It is denoted as $Sym(G)$ and is isomorphic to G. In other words, G and $B(G)$ are homomorphisms. The injective group between them maps each element g of G to the bijection on G by sending x to gx for all x in G. This homomorphism holds the property of injectivity because distinct elements of G are sent to distinct bijections of G, and it is a group homomorphism because it preserves the group operations formed by group G.

Remark. Consider the function $\tau_a: G \to G$ for $a \in G$, $\tau_a(x) = ax$ for $x \in G$. For $a, b \in G$, $(\tau_a * \tau_b)(x) = \tau_a(\tau_b(x)) = \tau_a(bx) = a(bx) = (ab)x = \tau_{ab}(x)$. Therefore, $\tau_a * \tau_b = \tau_{ab}$, and τ_a is bijective. It is noted that τ_a is injective because symmetric groups satisfy the identity. It implies that $g = g * e = e$ and $g = g'$. Thus, G is isomorphism with the subgroup S_n.

3. Application of Permutation Group on Rubik's cube

Rubik's cube is a longstanding untoward toy that has become an influential symbol ever since its invention in 1974. From a mathematical perspective, Rubik's cube is a fascinating object to study because it exhibits many interesting properties related to group theory [8].

Group theory studies the symmetry and structure in mathematical objects, and Rubik's cube is exactly such an example of group theory in action. The group of all possible cube configurations and the operations that can be used to manipulate it is known as the finite Rubik's cube group. It owns several interesting properties, including being non-commutative and having subgroups of various sizes. These properties make Rubik's cube an excellent object to study from a group theory perspective, as it can help researchers to better understand the fundamental properties of groups.

Suppose that the Rubik's cube is placed in a spatial rectangular coordinate system with the center at the origin and all edges are parallel to the axis. The faces of a Rubik's cube are named after directions of the normal vectors on the outside. The front (back) face is on the positive (negative) direction of the X-axis. Similarly, the left (right) face is on the positive (negative) direction of the Y-axis, while the up (down) face is on the positive (negative) direction of the Z-axis. For simplicity, the initial letters can be written as FBLRUD respectively (as illustrated in Fig. 1) [9].

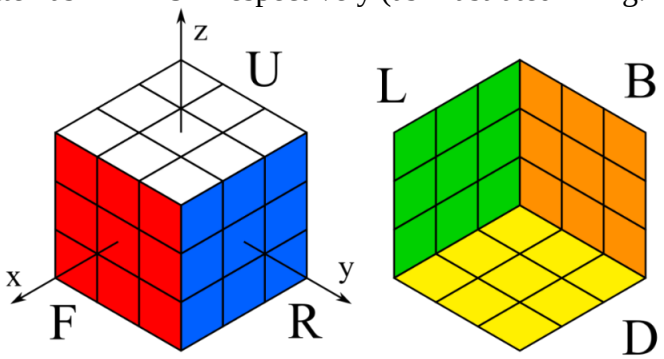

Figure 1. Coordinate system, title of surface and standard state

The state of a block is the sequence of faces at which its face is located. For example, a white, blue and red (WBR) corner block has the white side in front, the blue side in left, and the red side in the top, and the later is said to be in a state of "front upper left (FLU)" (see Fig 2, left panel). It is saying that "block a in state b" is referred as "a@b". The face sequence of the state name should correspond to the face sequence of the block name. Therefore, if the block is called "blue red white (BRW)", then the state should be called "left upper front (LUF)". That is, "WBR@FLU" has the same meaning as "BRW@LUF" but is different from "WBR@LUF" (see Fig 2, right panel). The location of a block is the set of faces at which its face is located. That is, the order (direction) is insignificant. The expression "block a in position b" is equivalent to "a ~ b". The same location can also have multiple names. For example, WBR@FLU has the same meaning as WBR@LUF.

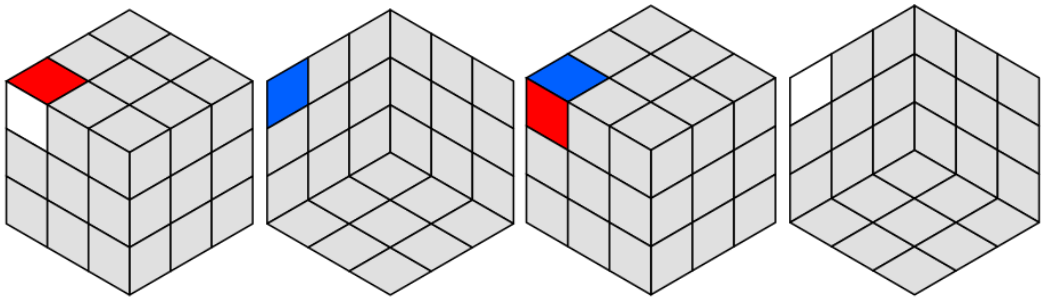

Figure 2. Left panel: WBR@FLU. Right panel: WBR@LUF

If one processes FFRR on a Rubik's cube, then a set of permutations should be achieved: (DF UF) (DR UR) (BR FR FL) (RB RF LF) (DBR UFR DFL) (BRD FRU FLD) (RDB RUF LDF) (ULF URB DRF) (LFU RBU RFD) (FUL BUR FDR). If people don't look at what the permutations exactly are

but just care how many permutations may occur, then one need to write this as: 2 (2) 8 (3), which means that second-order permutations occur twice, and third-order permutations occur eight times.

A Rubik's cube has 8 corner blocks, so the possibilities of variations of corner block positioning are $8!$. Each corner block has three orientations, so the total possibilities of variations of corner blocks are $8! \times 3^8$. Similarly, there are 12 edges and each edge has 2 directions, so the possibilities of variations of edges are $12! \times 2^{12}$. Therefore, if one arbitrarily assembles the Rubik's cube, the total possibilities of variation are $8! \times 3^8 \times 12! \times 2^{12}$ [10]. Since there is a half chance that the block is positioned correctly, a half chance that the edge is oriented correctly, and a third chance that the corner block is oriented correctly. Taken together, the total number of states to form a recoverable Rubik's cube is $\frac{8!\times 3^8\times 12!\times 2^{12}}{2\times 2\times 3}$. Noticing that a Rubik cube has 54 blocks, the set of total permutations to recover a Rubik's cube could be represented by the subgroup of permutation group S_{54}.

4. Conclusion

To conclude, this paper begins with an introduction to group theory, explaining what groups are, the properties that define them, and the various types of groups that exist. After that, the paper delves into the specific concepts of permutation groups by defining them, discussing their properties and operations, and exploring their applications to solve Rubik's cube. This work highlights some of the key theorems in group theory, including the famous Lagrange's theorem and Cayley's theorem, and explains how they can be applied to permutation groups. It also discusses different types of permutation groups, such as cyclic and symmetric groups, and provides examples of their applications in solving Rubik's cube. Overall, the article aims to provide readers with a foundational understanding of group theory and permutation groups. Meanwhile, it also highlights their practical applications to conquer some complicated objects such as the Rubik's cube.

References

[1] Dummit David, Foote Richard. Abstract algebra. Wiley, Vermont, 2004.

[2] Wang Efang. Fundamentals of finite group theory. Tsinghua University Press, 2002.

[3] Farahat H. K., Peel M. H. On the representation theory of the symmetric groups. Journal of Algebra, 1980, 67(2): 280-304.

[4] Cameron Peter J. and Semeraro Jason. The Cycle Polynomial of a Permutation Group. The Electronic Journal of Combinatorics, 2018, 25(1): 1-14.

[5] Gopalakrishnan Mini, Kumari N. Naga Maruthi. Generator graphs for cyclic groups. AIP Conference Proceedings, 2019, 2112(1): 020119.

[6] Mamidi Sai Akash. Applications Of Lagrange's Theorem in Group Theory. Int. J. Math. Comput. Sci., 2015, 3(8): 1150-1153.

[7] Graves-Morris P. R., Baker George A., Woodcock C. F. Cayley's theorem and its application in the theory of vector Padé approximants, J. Comput. Appl. Math, 1996, 66(1): 255-265.

[8] Joyner David. Adventures in group theory: Rubik's cube, Merlin's machine, and other mathematical toys. John Hopkins University Press, 2008.

[9] Shih K.-S. Weighted Permutations and the Group of the Rubik's Cube. Chinese Journal of Mathematics, 1981, 9(2): 65–78.

[10] Volte E., Patarin J., Nachef V. Zero knowledge with Rubik's cubes and non-abelian groups. Cryptology and Network Security, 2013, 8257: 74-91.