

Algebraic Modeling of Rubik's Cube with Group Theory

Chenyu Jia

Department of Mathematics, Xi'an Jiaotong Liverpool University, Suzhou, China
Chenyu.Jia23@student.xjtlu.edu.cn

Abstract. Transitioning from the practical manipulation of the Rubik's Cube to its theoretical abstraction presents significant challenges, compounded by a scarcity of foundational resources facilitating this shift. To address this gap and establish a theoretical basis for abstract Rubik's Cube analysis, this paper provides the fundamental methodology and key conclusions for constructing an algebraic model of the standard 3x3x3 Rubik's Cube using group theory. Cube operations are defined using the definition of a group, and the concept of the Rubik's Cube group is formally introduced. Employing knowledge of permutation groups, it is demonstrated that any state of the cube can be represented by an element within the set denoted by the direct product of four special groups. Subsequently, by employing group actions, this paper successfully integrates the Rubik's Cube group with the state space thereby completing the core algebraic modeling of the cube. Utilizing this model, the equivalence condition for solvable cube configurations: the sign of permutation in position of corner and edge are the same, and there was no single edge cube or corner cube artificially flipping. Finally, based on this equivalence, the number of solvable states for a standard 3x3x3 Rubik's Cube is found.

Keywords: Permutation group, Rubik's cube group, group action, direct product, reducible stat

1. Introduction

Group theory, pioneered by the French mathematician Évariste Galois in the nineteenth century, provides a rigorous abstract algebraic framework for characterizing symmetry. As a cornerstone of modern mathematics, this theory, through its quantitative unified language for symmetric structures, has profoundly reshaped multiple disciplines. The foundational significance of group theory cannot be overstated. As a revolutionary conceptual framework, it fundamentally reshaped the landscape of modern mathematics by providing the essential language to quantify and manipulate symmetry which is a universal principle governing both the natural and engineered worlds. Its axiomatic approach to structural invariance transcends specific applications, cementing its status as a cornerstone across scientific disciplines. Its significance extends beyond pure mathematics, forming an indispensable foundation for modern theoretical physics and crystallographic chemistry. The standard model of modern physics, Noether's theorem, or the study of crystal structures in modern chemistry are all based on group theory [1-4]. Crucially, symmetrical principles manifest not only in natural phenomena but also permeate engineered systems, underscoring the universality of group

theory. The Rubik's Cube, a quintessential combinatorial puzzle invented in the twentieth century, exemplifies such engineered symmetry. The state transitions it undergoes via scrambling and restoration are governed by discrete spatial symmetry operations, thereby establishing an essential pathway for rigorous mathematical analysis grounded in group-theoretic principles.

Previous research has formalized the state space and operational mechanics of the Rubik's Cube as the Rubik's Cube Group which is a well-defined permutation group structure [5]. Landmark work in the 1980s leveraged this model, combined with computational enumeration, to derive an upper bound of 20 moves for the minimal number of turns required to restore any arbitrary configuration; this constant was designated the "God's number" [6]. Its significance transcends merely solving a popular puzzle. It constitutes a profound validation of the theory's power and universality. Moreover, it vividly exemplifies how esoteric mathematical abstraction provides indispensable tools for dissecting and mastering complex real-world systems exhibiting constrained transformations. This successful modeling effort powerfully reinforces the profound interconnectedness between pure mathematical theory and the analysis of complex rule-based systems. It demonstrates the theory's unmatched capacity to reveal underlying order and optimal pathways beneath apparent chaos.

Although fundamental group-theoretic concepts such as permutation groups and commutators played pivotal roles in this achievement [7], a systematic exposition of the group-theoretic modeling methodology remains lacking in the existing literature. Current research mainly focuses on computational results, often neglecting pedagogical exposition of the underlying algebraic structures, resulting in a gap within the theoretical synthesis.

Therefore, this paper aims to bridge this gap by formally constructing the Rubik's Cube group. It places particular emphasis on elucidating the fundamental process of modeling the cube group theoretically and focuses sharply on the profound connections between core group-theoretic concepts, specifically permutation groups and group actions on Rubik's Cube.

The remainder of the paper is structured as follows: Section 2 details fundamental group theoretic concepts and theorems. Section 3 summarizes the algebraic formalization of the Rubik's Cube. Section 4 concludes the whole paper and outlines open theoretical challenges.

2. Preliminaries on group theory

Definition 2.1: A group is an ordered pair $(V, \cdot)$ where V is a set and $\cdot: V \times V \rightarrow V$ is a binary operation satisfying:

1. $(v \cdot w) \cdot t = v \cdot (w \cdot t)$ for all $(v, w, t \in V)$
2. There exists $(i \in V)$ such that $(i \cdot v = v \cdot i = i)$ for all $(v \in V)$
3. For every $(v \in V)$, there exists $(v^{-1} \in V)$ such that $(v \cdot v^{-1} = v^{-1} \cdot v = i)$

Proposition 2.1: Let V be a group and $(v, w, t \in V)$. Then:

$$\text{The identity } i \text{ is unique} \tag{1}$$

$$\text{The inverse } v^{-1} \text{ is unique} \tag{2}$$

$$(v^{-1})^{-1} = v \tag{3}$$

$$(v \cdot w)^{-1} = w^{-1} \cdot v^{-1} \tag{4}$$

$$v \cdot w = v \cdot t \Rightarrow w = t \text{ and } w \cdot v = t \cdot v \Rightarrow w = t \tag{5}$$

Proof:

1. Suppose i, i' are identities. Then $i = i \cdot i' = i'$

2. Suppose w, t are inverses of v . Then: $w = w \cdot i = w \cdot (v \cdot t) = (w \cdot v) \cdot t = i \cdot t = t$

3. Since $(v \cdot v^{-1} = v^{-1} \cdot v = i)$, v satisfies the inverse condition for v^{-1} .

4. Compute: $(v \cdot w) \cdot (w^{-1} \cdot v^{-1}) = v \cdot (w \cdot w^{-1}) \cdot v^{-1} = v \cdot e \cdot v^{-1} = v \cdot v^{-1} = i$

Similarly, $(w^{-1} \cdot v^{-1}) \cdot (v \cdot w) = i$

5. Left-multiply $(v \cdot w = v \cdot t)$ by (v^{-1}) :
 $v^{-1} \cdot (v \cdot w) = v^{-1} \cdot (v \cdot t) \Rightarrow (v^{-1} \cdot v) \cdot w = (v^{-1} \cdot v) \cdot t \Rightarrow i \cdot w = i \cdot t \Rightarrow w = t$

Right cancellation follows symmetrically.

Definition 2.2. A subset $H \subseteq V$ is a subgroup of V (denoted $H \leq V$) if:

$$i \in H \quad (6)$$

$$v, w \in H \Rightarrow v \cdot w \in H \quad (7)$$

$$v \in H \Rightarrow v^{-1} \in H \quad (8)$$

Proposition 2.2. A nonempty subset $(H \subseteq V)$ is a subgroup iff $(\forall \nu, \omega \in H), (\nu \cdot \omega^{-1} \in H)$.

Proof:

$(\Rightarrow)$ If H is a subgroup and $\nu, \omega \in H$, then $\omega^{-1} \in H$ and $\nu \cdot \omega^{-1} \in H$ by Definition 2.2.

$(\Leftarrow)$ Since $H \neq \emptyset$, fix $\nu \in H$. Then $e = \nu \cdot \nu^{-1} \in H$. For any $\omega \in H, \omega^{-1} = e \cdot \omega^{-1} \in H$.

For closure: given $\nu, \omega \in H, \omega^{-1} \in H$ implies $\nu \cdot (\omega^{-1})^{-1} = \nu \cdot \omega \in H$

Definition 2.3. A group V acts on a set Ω if there exists a map $(\varphi : V \times \Omega \rightarrow \Omega)$ (denoted $(g \cdot \xi)$) such that:

$$e \cdot \xi = \xi \text{ for all } \xi \in \Omega \quad (9)$$

$$g_1 \cdot g_2 \cdot \xi = g_1 \cdot (g_2 \cdot \xi) \text{ for all } g_1, g_2 \in V, \xi \in \Omega \quad (10)$$

Definition 2.4. The symmetric group S_η is the group of all bijections $\sigma : \{1, \dots, \eta\} \rightarrow \{1, \dots, \eta\}$ under function composition.

Definition 2.5. A κ -cycle $(\xi_1 \xi_2 \dots \xi_\kappa)$ denotes the permutation satisfying:

$$\xi_\iota \mapsto \xi_{\iota+1} \ (1 \leq \iota < \kappa), \quad \xi_\kappa \mapsto \xi_1 \quad (11)$$

with all other elements fixed. A 2-cycle is called a transposition.

Proposition 2.3. Every $\sigma \in S_\eta$ decomposes uniquely (up to cycle ordering) into disjoint cycles.

Proof:

Define an equivalence relation on $\{1, \dots, \eta\}$ by $\iota \sim j$ iff $j = \sigma^\lambda(\iota)$ for some $\lambda \in \mathbb{Z}$. The equivalence classes partition $\{1, \dots, \eta\}$, and σ restricted to each class is a cycle. Uniqueness follows from the orbit structure of $\langle \sigma \rangle$.

Definition 2.6. The sign of $\sigma \in S_\eta$ is $\text{sgn}(\sigma) = (-1)^\mu$ where μ is the minimal number of transpositions in any decomposition of σ . A permutation is even if $\text{sgn}(\sigma)=1$, odd if $\text{sgn}(\sigma)=-1$.

Proposition 2.4. For $(\sigma, \tau \in S_\eta)$:

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \text{sgn}(\tau) \quad (12)$$

$$\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma) \quad (13)$$

$$\text{sgn}(\xi_1 \xi_2 \dots \xi_\kappa) = (-1)^{\kappa-1} \quad (14)$$

Proof:

1. Let $\sigma = \tau_1 \dots \tau_\ell$ and $\tau = \tau'_1 \dots \tau'_\varsigma$ be minimal transposition decompositions. Then $\sigma\tau = \tau_1 \dots \tau_\ell \tau'_1 \dots \tau'_\varsigma$ gives $\text{sgn}(\sigma\tau) = (-1)^{\ell+\varsigma} = (-1)^\ell (-1)^\varsigma = \text{sgn}(\sigma) \text{sgn}(\tau)$.
2. $\text{sgn}(\sigma) \text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma\sigma^{-1}) = \text{sgn}(i) = (-1)^0 = 1$.
3. The κ -cycle decomposes as $(\xi_1 \xi_\kappa)(\xi_1 \xi_{\kappa-1}) \dots (\xi_1 \xi_2)$ ($\kappa-1$ transpositions). Minimality follows from $\text{sgn}(i) = 1 \neq (-1)^\kappa$ for $\kappa > 1$.

Definition 2.7 The direct product of groups $V_1, \dots, V_\kappa$ is $V_1 \times \dots \times V_\kappa$ with operation:

$$(v_1, \dots, v_\kappa) \cdot (w_1, \dots, w_\kappa) = (v_1 w_1, \dots, v_\kappa w_\kappa) \quad (15)$$

For group A and $\eta \in \mathbb{Z}^+$, define $A^\eta = \underbrace{A \times \dots \times A}_{\eta \text{ times}}$.

Definition 2.8. The cyclic group of order η is $\mathbb{Z}/\eta\mathbb{Z} = \{0, 1, \dots, \eta-1\}$ with addition modulo η .

Proposition 2.5 In $\mathbb{Z}/\eta\mathbb{Z}$:

1. The element κ has order $\eta/\text{gcd}(\kappa, \eta)$
2. Subgroups are cyclic of order δ where $\delta \mid \eta$

Proof:

1. The order is the minimal $\mu > 0$ such that $\mu\kappa \equiv 0 \pmod{\eta}$, i.e., $\eta \mid \mu\kappa$. This is $\mu = \eta/\text{gcd}(\kappa, \eta)$.
2. Let $H \leq \mathbb{Z}/\eta\mathbb{Z}$. If $H = \{0\}$, done. Else let $\delta = \min\{\kappa \in \mathbb{Z}^+ : \kappa \bmod \eta \in H \setminus \{0\}\}$. Then $H = \langle \delta \rangle$, and $\delta \mid \eta$ since $\eta \equiv 0 \in H$.

3. Modeling the Rubik's Cub

Assumption 3.1. Subsequent discussions refer specifically to the standard $3 \times 3 \times 3$ Rubik's Cube. The spatial orientation of the cube remains fixed during operations.

Definition 3.1. Fundamental moves are defined as clockwise 90° rotations of each face:

- U: Upper face rotation
- D: Down face rotation
- R: Right face rotation
- L: Left face rotation
- F: Front face rotation
- B: Back face rotation

Definition 3.2. Let W denote the set generated by arbitrary compositions of moves $\{U, D, R, L, F, B\}$. Elements of W are denoted w and termed valid operations.

Theorem 3.1. $(R, \circ)$ forms a group under operation composition, termed the Rubik's Cube Group

Proof:

Associativity: $\forall r_1, r_2, r_3 \in R$,

$$(r_1 \circ r_2) \circ r_3 = r_1 \circ (r_2 \circ r_3) \quad (16)$$

Identity element : $\exists U^4 \in R$ such that $\forall r \in R$,

$$r \circ U^4 = U^4 \circ r = r \quad (17)$$

Inverse element : Obviously $U^{-1} = U^3$, with analogous inverses for R, L, D, F, B.

Since each basic move has an inverse element, their composite must also have an inverse element: we only need to reverse the order and execute the corresponding inverse element in sequence. Which means for all $r^{-1} \in R$ satisfying:

$$r \circ r^{-1} = r^{-1} \circ r = i \quad (18)$$

Definition 3.3. According to the construction of the Rubik's Cube, there are a total of 48 color blocks with adjustable positions. This paper refers to the set of 48 color blocks arranged arbitrarily as state set X. This paper have defined valid operations in Definition 3.3, and we call all states that can be obtained from valid operations valid states, and non valid states invalid states. The operation that can obtain an invalid state is called an invalid operation.

Theorem 3.2 $(R, \circ)$ is a subgroup of $(S_{48}, \circ)$.

Proof:

Each $r \in R$ permutes 48 facelets $\Rightarrow R \hookrightarrow S_{48}$

R is a group (Theorem 3.1)

Thus $R \leq S_{48}$

Definition 3.4. Orientation assignment:

The following contents define the orientation of each cube

Corner cubes

Assuming that each cube at front-down-left position:

0 : down face

1 : left face

2 : front face

Edge cubes

Assuming that each cube at front-left position:

0 : left face

1 : front face

This paper defines the upper and down surfaces of all corner cube positions as the positive direction. The upper, down, front, and back surfaces of the edge cube are defined as positive directions. Then the orientation of the cube is defined as the number that coincides with the positive direction

Definition 3.5. Position indexing:

The following contents define the position of each cube

Corner positions:

– Top layer: 1 (front-up-left), 2 (front-up-right), 3 (back-up-right), 4 (back-up-left)

– Bottom layer: 5 (down-back-left), 6 (down-front-left), 7 (down-front-right), 8 (downback-right)

Edge positions:

– Top layer: 1 (up-back), 2 (up-right), 3 (up-front), 4 (up-left)

- Middle layer: 5 (back-left), 6 (back-right), 7 (front-right), 8 (front-left)
- Bottom layer: 9 (down-back), 10 (down-right), 11 (down-front), 12 (down-left)

Theorem 3.3. Any cube state is uniquely determined by:

Corner positions $\varsigma \in S_8$

Edge positions $\varrho \in S_{12}$

Corner orientations $\kappa \in (\mathbb{Z}/3\mathbb{Z})^8$

Edge orientations $\zeta \in (\mathbb{Z}/2\mathbb{Z})^{12}$

$$\text{Thus : } State = (\varsigma, \varrho, \kappa, \zeta) \in S_8 \times S_{12} \times (\mathbb{Z}/3\mathbb{Z})^8 \times (\mathbb{Z}/2\mathbb{Z})^{12} =: X \quad (19)$$

Proof:

If the Rubik's Cube has two states which all four conditions are the same, then their states must also be the same.

Theorem 3.4. Twisting Rubik's Cube in real life can be modeled as the following group action

$$P : R \times X \rightarrow X \text{ where } P(r, x) = r \cdot x$$

This symbol defined as the state obtained by twisting a Rubik's Cube with an initial state of r using R

Proof: Based on intuition from reality

$$(r_1 \circ r_2) \cdot x = r_1 \cdot (r_2 \cdot x) \quad (20)$$

$$U^4 \cdot x = x \quad \forall x \in X \quad (21)$$

Theorem 3.5. Fundamental moves which are U,D,F,R,L,B, induce these permutations in Table 1:

Table 1. The permutations of fundamental moves

Operation	Positional Permutation	Orientation Change
U	Corners: (2 1 4 3) Edges: (1 2 3 4)	$\kappa : (\kappa_2, \kappa_3, \kappa_4, \kappa_1, \kappa_5, \kappa_6, \kappa_7, \kappa_8)$
		$\zeta : (\zeta_4, \zeta_1, \zeta_2, \zeta_3, \zeta_5, \zeta_6, \zeta_7, \zeta_8, \zeta_9, \zeta_{10}, \zeta_{11}, \zeta_{12})$
D	Corners: (5 6 7 8) Edges: (11 10 9 12)	$\kappa : (\kappa_1, \kappa_2, \kappa_3, \kappa_4, \kappa_8, \kappa_5, \kappa_6, \kappa_7)$
		$\zeta : (\zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_5, \zeta_6, \zeta_7, \zeta_8, \zeta_{10}, \zeta_{11}, \zeta_{12}, \zeta_9)$
R	Corners: (2 3 8 7) Edges: (2 6 10 7)	$\kappa : (\kappa_1, \kappa_7 + 1, \kappa_2 + 2, \kappa_4, \kappa_5, \kappa_6, \kappa_8 + 2, \kappa_3 + 1)$
		$\zeta : (\zeta_1, \zeta_7, \zeta_3, \zeta_4, \zeta_5, \zeta_2, \zeta_{10}, \zeta_8, \zeta_9, \zeta_6, \zeta_{11}, \zeta_{12})$
L	Corners: (1 6 5 4) Edges: (4 8 12 5)	$\kappa : (\kappa_4 + 2, \kappa_2, \kappa_3, \kappa_5 + 1, \kappa_6 + 2, \kappa_1 + 1, \kappa_7, \kappa_8)$
		$\zeta : (\zeta_1, \zeta_2, \zeta_3, \zeta_5, \zeta_{12}, \zeta_6, \zeta_7, \zeta_4, \zeta_9, \zeta_{10}, \zeta_{11}, \zeta_8)$
F	Corners: (1 2 7 6) Edges: (3 7 11 8)	$\kappa : (\kappa_6 + 1, \kappa_1 + 2, \kappa_3, \kappa_4, \kappa_5, \kappa_7 + 2, \kappa_2 + 1, \kappa_8)$
		$\zeta : (\zeta_1, \zeta_2, \zeta_8 + 1, \zeta_4, \zeta_5, \zeta_6, \zeta_3 + 1, \zeta_{11} + 1, \zeta_9, \zeta_{10}, \zeta_7 + 1, \zeta_{12})$
B	Corners: (3 4 5 8) Edges: (1 5 9 6)	$\kappa : (\kappa_1, \kappa_2, \kappa_8 + 1, \kappa_3 + 2, \kappa_4 + 1, \kappa_6, \kappa_7, \kappa_5 + 2)$
		$\zeta : (\zeta_6 + 1, \zeta_2, \zeta_3, \zeta_4, \zeta_1 + 1, \zeta_9 + 1, \zeta_7, \zeta_8, \zeta_5 + 1, \zeta_{10}, \zeta_{11}, \zeta_{12})$

Theorem 3.6. A scrambled cube state $(\varsigma, \varrho, \kappa, \zeta) \in X$ is valid (solvable) if and only if:

$$\text{sgn}(\varsigma) = \text{sgn}(\varrho) \quad (22)$$

$$\sum_{i=1}^8 \kappa_i \equiv 0(\text{mod}3), \quad \sum_{j=1}^{12} \zeta_j \equiv 0(\text{mod}2) \quad (23)$$

Proof:

Part (1) sufficiency:

By Theorem 3.5, each fundamental operation (U, F, D, B, R, L) induces an even permutation (product of 4-cycles) on both corner and edge positions. For any valid operation $r \in R$ composed of κ fundamental moves:

$$\text{sgn}(\varsigma) = \text{sgn}(\varrho) = (-1)^\kappa \quad (24)$$

Thus $\text{sgn}(\varsigma) = \text{sgn}(\varrho)$ holds for all reachable states.

The orientation conditions follow directly from the transition rules in Table 1 (Theorem 3.5), which preserve the invariant sums modulo 3 (corners) and 2 (edges) under all fundamental

operations.

Part (2) necessity:

A complete rigorous proof is available in reference [8].

Corollary 3.1. The physical interpretation of Theorem 3.6 is: A scrambled Rubik's Cube can be restored if only if the sign of permutation in position of corner and edge are the same, and there was no single edge cube or corner cube artificially flipping.

Theorem 3.7. The total number of solvable states is $(3^8 \cdot 8! \cdot 2^{12} \cdot 12!)/12$

Proof:

By Theorem 3.3, the combinatorial upper bound is: $3^8 \cdot 8! \cdot 2^{12} \cdot 12!$

accounting for:

- $8!$ corner position arrangements
- 3^8 possible corner orientations
- $12!$ edge position arrangements
- 2^{12} possible edge orientations

Applying Theorem 3.6 constraints:

Position parity: $\text{sgn}(\varsigma) = \text{sgn}(\varrho)$ eliminates half the configurations since odd permutation and even permutation are equally numerous

Corner orientation: $\sum \kappa_i \equiv 0 \pmod{3}$ eliminates 2/3 of configurations (lack 1 free orientation variable)

Edge orientation: $\sum \zeta_j \equiv 0 \pmod{2}$ eliminates half the configurations (lack 1 free orientation variable)

The constraints are independent, so the fraction of solvable states is:

$$\frac{1}{2} \times \frac{1}{3} \times \frac{1}{2} = \frac{1}{12} \quad (25)$$

Thus the total solvable states are:

$$\frac{1}{12} (3^8 \cdot 8! \cdot 2^{12} \cdot 12!) \quad (26)$$

4. Conclusion

This paper establishes an algebraic model for the standard $3 \times 3 \times 3$ Rubik's Cube using group theory, laying the groundwork for theoretical investigations. Employing permutation groups to define the states of the cube and the recoverable states. Fundamental operations on the cube are rigorously defined using concepts from group theory. Furthermore, unifying cube operations with their resulting state changes through the application of group actions. This approach not only completes the modeling of the standard cube but also advances to derive the conditions for recoverability and the total number of recoverable states. However, the scope of this study is confined to the $3 \times 3 \times 3$ cube. While the methodology can be naturally generalized mathematically to arbitrary $n \times n \times n$ cubes, modeling non-cubic puzzles such as regular polyhedral cubes or heartshaped cubes necessitates alternative approaches. Future work will focus on conducting deeper algebraic modeling studies of these irregular puzzles.

References

- [1] Ananthanarayan, B., Das, S., Lahiri, A. et al. (2024) Group theory in physics: an introduction with mathematics. Eur. Phys. J. Spec. Top., 233, 1443–1513.

- [2] Ramadevi, P. and Dubey, V. (2019) Group Theory for Physicists: With Applications. Cambridge University Press, Cambridge.
- [3] Fonseca, Q.M. (2021) Comput. Phys. Commun. 267, 108085.
- [4] Gururajan, M.P. (2019) Symmetry Relationships between Crystal Structures: Applications of Crystallographic Group Theory in Crystal Chemistry. Contemporary Physics, 60, 83–84.
- [5] Comock, C. (2015) Teaching group theory using Rubik's Cubes. International Journal of Mathematical Education in Science and Technology, 46, 957–967.
- [6] Joyner, D. (2014) The man who found God's number. The College Mathematics Journal, 258-266.
- [7] Sun, T. (2023) Commutators in the Rubik's Cube Group. The American Mathematical Monthly, 131, 3–19.
- [8] Chen, J. (2007) Group theory and the Rubik's cube. Harvard University.