Proceedings of CONF-APMM 2026 Symposium: Applied Mathematics and Quantitative Modeling
DOI: 10.54254/2753-8818/2026.PU37671

The Rubik's Cube Group: Structure, Commutators, and Algebraic Solving Strategies

Zihan Liu

Department of Mathematics and Statistics, University of North Carolina at Wilmington, Wilmington, USA
zl7011@uncw.edu

Abstract. The Rubik's Cube was invented by Ernő Rubik as a toy and has long served as a fertile ground for mathematical inquiry, particularly within finite group theory. This natural correspondence between a tangible puzzle and an abstract algebraic structure bridges intuition and formalism, establishing cube groups as canonical examples in both pedagogical and research-oriented algebra. Over the past five decades, extensive research has been devoted to understanding the group-theoretic structure of the Cube. Early investigations established the algebraic decomposition of cube groups via semidirect products, while subsequent work explored generators and relations, the diameter of the Cayley graph, and configuration enumeration. More recently, representation theory and the commutator structure of cube groups have emerged as frontiers, with significant results on minimal representation dimensions and the proof that every element of the commutator subgroup is itself a single commutator. The present paper surveys these group-theoretic foundations underlying Rubik's Cube modeling and solving strategies. It recapitulates essential preliminaries and then focuses on two complementary modelling approaches: the first employs linear algebra and permutation group theory to develop a mathematical reduction model, and the second examines the specific role of commutators in blindfolded solving. The paper concludes with a discussion of future research directions.

Keywords: Cube, Group Theory, Commutator

1. Introduction

The Rubik's Cube has long served as a fertile ground for mathematical inquiry, particularly in finite group theory that encodes the fundamental combinatorial constraints of the cube [1]. This natural correspondence between a tangible puzzle and an abstract algebraic structure bridges intuition and formalism, establishing the cube groups as canonical examples in both pedagogical and research-oriented algebra [2]. Zassenhaus [3] notably described the cube as "the most important tool for the group-theoretician" due to the wide range of concepts including subgroups, generators, orbits, and conjugacy that can be demonstrated on it.

Over the past five decades, extensive research has been devoted to understanding the group-theoretic structure of the Rubik's Cube. Early investigations established the algebraic decomposition of cube groups as semidirect products of position and orientation subgroups, expressed as

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-8818/2026.PU37671

$G \cong (\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}) \rtimes (S_8 \times S_{12})$ modulo parity constraints [4]. Subsequent work explored generators and relations, the Cayley graph diameter culminating in the determination of "God's number" as 20 [5, 6], and the enumeration of configurations via the Pólya–Burnside lemma [7]. More recently, the representation theory of cube groups has emerged as a frontier. Daly and Kingsnorth determined the minimal faithful complex representation dimensions for the 2×2 and 3×3 cube groups [8], showing that G_2 admits a minimal representation of dimension 8, while G_3 requires dimension 20. The commutator structure of the cube group has also received sustained attention; Sun recently proved that every element of the commutator subgroup corresponding to half of all solvable positions is itself equal to a single commutator [9], resolving a long-standing question at the interface of group theory and cubing practice. These achievements have collectively established cube groups as canonical objects in computational group theory and representation theory, with applications extending to the study of finite group invariants and algorithmic symmetric reduction [8].

The present paper surveys the group-theoretic foundations underlying Rubik's Cube modeling and solving strategies. The remainder of the paper is organized as follows. Section 2 recapitulates essential group-theoretical preliminaries and notation. Section 3 focuses on two complementary modelling approaches. To be more specific, the present study firstly employs linear algebra and group theory including permutations, conjugacy, and commutators to develop a mathematical reduction model for the cube [9]. Second, the specific role of commutators in blindfolded solving is examined, demonstrating how the identity $[X, Y] = XYX^{-1}Y^{-1}$ enables the construction of three-cycles that form the backbone of memory-based strategies [10]. Finally, Section 4 concludes with future research directions [3].

2. Group-theoretical preliminaries and notation

2.1. Groups and subgroups

Definition 2.1. A group is a nonempty set G equipped with a binary operation:

$$G \times G \to G \tag{1}$$

satisfying the following axioms:

1. Associativity: $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ for all $\alpha, \beta, \gamma \in G$;
2. Identity: There exists $e \in G$ such that $e \cdot \alpha = \alpha \cdot e = \alpha$ for all $\alpha \in G$;
3. Inverses: For each $\alpha \in G$, there exists $\beta \in G$ such that $\alpha \cdot \beta = \beta \cdot \alpha = e$.

If $\alpha \cdot \beta = \beta \cdot \alpha$ for all $\alpha, \beta \in G$, the group is called abelian (or commutative); otherwise, it is non-abelian.

Definition 2.2. A nonempty subset $F \subseteq G$ *is a subgroup of* G, denoted $F \leq G$, if F is itself a group under the restriction of the operation of G. If $F \leq G$ and $fHf^{-1} \subseteq F$ for all $f \in G$, then F is a normal subgroup, denoted $F \triangleright G$.

Definition 2.3. For a subset $S \in G$, the subgroup generated by S is the intersection of all subgroups of G containing S, denoted $\langle S \rangle$. If $G = \langle S \rangle$, then S is a generating set for G, and its elements are called generators.

In the Rubik's Cube group, the six face rotations R, U, F, B, L, D constitute a natural generating set. The group is non-abelian, as can be verified by comparing the effect of RU and UR on the cube.

DOI: 10.54254/2753-8818/2026.PU37671

2.2. Permutations and the symmetric group

Definition 2.4. Let T be a finite set. A permutation of T is a bijection $\sigma : T \to T$. The set of all permutations of T, equipped with composition as the group operation, forms the symmetric group S_T. When $T = \{1,2,\ldots,n\}$, this group is denoted S_n.

Cycle notation: A permutation $\sigma \in S_n$ is written in cycle notation like $(a_1\ a_2 \ldots a_k)$, meaning $\sigma(a_i) = a_{i+1}$ for $1 \le i < k$ and $\sigma(a_k) = a_1$. Elements not appearing in a cycle are fixed. A cycle of length 2 is called a transposition. Every permutation decomposes uniquely (up to cyclic rotation of the entries within each cycle) as a product of disjoint cycles.

Example 2.5. The permutation sending 1↦2, 2↦3, 3↦1, 4↦5, 5↦4 is written (1 2 3)(4 5).

Definition 2.6. A permutation that can be written as a product of an even number of transpositions is an even permutation; otherwise, it is odd. The parity of a permutation is well-defined, independent of the decomposition. The set of all even permutations forms a normal subgroup belong to S_n called the alternating group A_n. Since $[S_n : A_n] = 2$, it follows that $|A_n| = \frac{n!}{2}$.

Lemma 2.7 (Generation by 3-cycles). The alternating group A_n is generated by 3-cycles ($\alpha\,\beta\,\gamma$). Moreover, the 3-cycles of the form $(1\ 2\ k)$ for $3 \le k \le n$ already suffice.

This lemma is fundamental to the construction of cube-solving algorithms: once 3-cycles on arbitrary positions can be produced, every even permutation becomes accessible. For the cube, the parity constraint (cf. Section 3.2) restricts the group to even permutations of the cubies, making 3-cycles the primary building blocks.

2.3. Group actions

Definition 2.8. A left action of a group A on a set B is a map $A \times B \to B$, denoted $(a, b) \mapsto a \cdot b$, satisfying:

1.$e \cdot b = b$ for all $b \in B$;

2.$(ac) \cdot b = a \cdot (c \cdot b)$ for all $a, c \in A$ *and* $b \in B$.

Definition 2.9. For a given action, $\mathcal{O}x = \{g \cdot x : g \in G\}$ is the orbit of $x \in X$, and $Stab_G(x) = \{g \in G : g \cdot x = x\}$ is the stabilizer of x .

The Orbit-Stabilizer Theorem is: $|\ \mathcal{O}x\ | = |\ G\ |\ /\ |\ Stab_G(x)\ |$.

An action is transitive when it consists of a single orbit, and faithful when the induced homomorphism $G \to S_X$ is injective. Equivalently $\bigcap_{x \in X} Stab_G(x) = \{e\}$.

In the cube setting, the group acts naturally on the set of corner positions, on the set of edge positions, and on the set of facelets. The action on positions is transitive but not faithful (central rotations of the entire cube fix all positions but move facelets), whereas the action on oriented cubies is faithful.

2.4. Semidirect products

The semidirect product provides the algebraic framework for describing how position permutations and orientation twists couple in the Rubik's Cube group.

Definition 2.10. Let F and G be groups, and let $\varphi : G \to Aut(F)$ be a homomorphism. The semidirect product $F \rtimes_\varphi G$ is the set $F \times G$ equipped with multiplication

DOI: 10.54254/2753-8818/2026.PU37671

$$(f_1, g_1)(f_2, g_2) = (f_1 \varphi_{g1}(f_2), g_1 g_2) \tag{2}$$

where φ_{g1} denotes the automorphism $\varphi(g1)$ applied to f_2 . The identity is (e_F, e_G) and the inverse of (f, g) is $(\varphi_{g^{-1}}(f^{-1}), g^{-1})$.

Remark 2.11. When φ is the trivial homomorphism ($\varphi g = id_G$ for all $g \in G$), the semidirect product reduces to the ordinary direct product $F \times G$. The semidirect product is therefore a generalization that encodes nontrivial actions of G on F.

Lemma 2.12 (Recognition criterion). Let G be a group with $N \lhd G$ and $H \leq G$. If $G = NH$ and $N \cap H = \{e\}$, then $G \cong N \rtimes_{\varphi} H$, where $\varphi h(n) = hnh^{-1}$.

This criterion applies directly to the Rubik's Cube: the normal subgroup of orientation-preserving transformations and the subgroup of pure position permutations satisfy the conditions, yielding the semidirect decomposition.

2.5. Commutators and conjugacy

Definition 2.13. For $X, Y \in G$, the commutator of X and Y is

$$[X, Y] = XYX^{-1}Y^{-1} . \tag{3}$$

Two elements commute if and only if $[X, Y] = e$. The commutator quantifies the extent to which X and Y fail to commute. In practice, commutators are the principal tool for constructing local operations. The heuristic principle is as follows: if X and Y have overlapping but not identical supports (the sets of pieces they affect), then their commutator tends to affect only the overlap region, often producing a 3-cycle.

Definition 2.14. The conjugate of $X \in G$ by $P \in G$ is PXP^{-1} . Conjugation preserves all structural properties of X : it has the same order and the same cycle structure, but its action is "relocated" to the image under P of the original support. Consequently, once a commutator producing a 3-cycle on one set of positions has been found, arbitrary conjugates can be used to produce 3-cycles on any other set of positions.

2.6. Elementary abelian groups and automorphisms

Definition 2.15. The group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is the additive group of integers modulo m. In cube modeling, $\mathbb{Z}_3$ encodes the three possible orientations of a corner cubie, and $\mathbb{Z}_2$ encodes the two possible orientations of an edge cubie. The direct products $\mathbb{Z}_3^8$ and $\mathbb{Z}_2^{12}$ represent the orientation state spaces of all corners and edges, respectively.

Vector convention. An element $v = (v_1, \ldots, v_8) \in \mathbb{Z}_3^8$ records the orientation of each corner cubie, with entries in $\{0,1,2\}$. Similarly, $w = (w_1, \ldots, w_{12}) \in \mathbb{Z}_2^{12}$ records edge orientations.

For a permutation $\sigma \in S_8$, its natural action on $v \in \mathbb{Z}_3^8$ is coordinate permutation:

$$(\sigma \cdot v)i = v_{\sigma^{-1}(i)} \tag{4}$$

DOI: 10.54254/2753-8818/2026.PU37671

The inverse indexing ensures that $(\sigma\tau)\cdot v = \sigma\cdot(\tau\cdot v)$, making this a genuine left action. The analogous action of S_{12} on $\mathbb{Z}_2^{12}$ is defined identically. This action defines homomorphisms $S_8 \to Aut(\mathbb{Z}_3^8)$ and $S_{12} \to Aut(\mathbb{Z}_2^{12})$, which are essential for formulating the semidirect product structure of the cube group.

3. Algebraic modeling of the Rubik's Cube introduction

This section develops the mathematical framework for modeling the Rubik's Cube. The first approach employs linear algebra and permutation group theory to establish a structural model of the cube group. The second examines the role of commutators in blindfolded solving, demonstrating how $[X\ ,\ Y] = XYX^{-1}Y^{-1}$ enables the construction of three-cycles.

3.1. State representation

A Rubik's Cube configuration is determined by:

1. The permutation of 8 corners: $\sigma_c \in S_8$;
2. The permutation of 12 edges: $\sigma_e \in S_{12}$;
3. The orientation of each corner: $c \in \mathbb{Z}_3^8$;
4. The orientation of each edge: $e \in \mathbb{Z}_2^{12}$.

3.2. The cube group and its semidirect product structure

Let G be the group of all reachable configurations. The six face rotations R, U, F, B, L, D generate G.

Theorem 3.1. The cube group decomposes as

$$G \cong (\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}) \rtimes (S_8 \times S_{12}), \tag{5}$$

where $S_8 \times S_{12}$ acts on $\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}$ by permuting coordinates according to cubie movement.

Explanation. The semidirect product is not a direct product because position and orientation are coupled: when a cubie moves, its orientation moves with it. This coupling is precisely encoded by the semidirect product multiplication:

$$(n_1, h_1)(n_2, h_2)(n_1, \varphi_{h_1}(n_2)\ h_1h_2)$$

where φ_{h_1} permutes orientation coordinates according to the position permutation h_1.

3.3. Parity constraints

Proposition 3.2 (Three invariants). For any reachable state:

1.Orner twist:

DOI: 10.54254/2753-8818/2026.PU37671

$$\sum c_i \equiv 0 \pmod 3 \tag{6}$$

2.Edge flip:

$$\sum e_i \equiv 0 \pmod 2 \tag{7}$$

3.Position parity:

$$\operatorname{sgn}(\sigma_c) = \operatorname{sgn}(\sigma_e) \tag{8}$$

Proof sketch. Each face rotation affects four corners (adding the same twist to all) and four edges (flipping all), changing each sum by a multiple of the modulus. For parity, a quarter-turn induces a 4-cycle on both corners and edges, so both permutations change sign simultaneously. Thus, these invariants are preserved by all generators.

Corollary 3.3. The number of reachable states is

$$\mid G \mid = \frac{3^8 \cdot 2^{12} \cdot 8! \cdot 12!}{3 \cdot 2 \cdot 2} = 43{,}252{,}003{,}274{,}489{,}856{,}000. \tag{9}$$

3.4. Linear algebra of face rotations

Each face rotation acts as an affine transformation on the orientation space $\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}$. For example, the R rotation acts as

$$R \cdot (c, e) = (\sigma_R(c) + \Delta_R^c, \sigma_R(e) + \Delta_R^e), \tag{10}$$

where σ_R permutes coordinates, and $\Delta_R^c \in \mathbb{Z}_3^8$, $\Delta_R^e \in \mathbb{Z}_2^{12}$ are fixed vectors encoding the twist/flip applied to affected cubies. Addition is componentwise modulo 3 or 2.

Thus, the entire cube group can be viewed as a subgroup of the affine group generated by six affine transformations corresponding to the face rotations. This formulation is suitable for computational implementation.

3.5. Commutators and three-cycles

3.5.1. The commutator identity

For operations X, Y, the commutator is

$$[X\ ,\ Y] = XYX^{-1}Y^{-1}. \tag{11}$$

DOI: 10.54254/2753-8818/2026.PU37671

If X and Y overlap only slightly in the cubies they affect, their commutator produces a local operation affecting only the overlap region.

3.5.2. Constructing three-cycles

Lemma 3.4. Let X affect a single cubie a, and let Y move a to b while fixing everything else. Then $[X\ ,\ Y]$ acts as a three-cycle $(a\ b\ c)$ for some c.

Example 3.5. With $X = RUR^{-1}$ and $Y = D$,

$$[RUR^{-1}, D] = (RUR^{-1})D(RUR^{-1})^{-1}D^{-1} \tag{12}$$

produces a three-cycle on three corners.

Once a three-cycle $C = (a\ b\ c)$ is obtained, conjugation relocates it to any other positions:

$$PCP^{-1} = (P(a)\ P(b)\ P(c)). \tag{13}$$

Thus, a single commutator-generated three-cycle, combined with arbitrary conjugations, yields three-cycles on any desired set of cubies.

3.5.3. Why three-cycles suffice

Theorem 3.5. The alternating group A_n is generated by three-cycles.

Proof. Every even permutation is a product of pairs of transpositions. A pair of transpositions factors as:

$(\alpha\ \beta)(\alpha\ \gamma) = (\alpha\ \gamma\ \beta)$ (a three-cycle);

$(\alpha\ \beta)(\gamma\ \delta) = (\alpha\ \delta\ \beta)(\alpha\ \gamma\ \beta)$ (product of two three-cycles).

So, any even permutation is a product of three cycles.

Since the parity constraint restricts the cube group to even permutations, every reachable cubie permutation can be achieved using only commutator-generated three-cycles.

3.6. Application to blindfolded solving

If the permutation parity is odd, the solver applies a single quarter-turn (an odd permutation), then proceeds with three-cycles. This matches the fact that A_n has index 2 in S_n, and the cube group lies in the diagonal parity subgroup.

4. Conclusion

This paper has surveyed the group-theoretic foundations underlying the Rubik's Cube, demonstrating how a concrete combinatorial puzzle gives rise to a rich algebraic structure. The semidirect product decomposition provides a rigorous framework for capturing the coupling between position permutations and cubie orientations, while the three parity invariants precisely characterize the set of reachable configurations. The commutator structure, in particular, emerges as the central mechanism for constructing local three-cycles, which in turn generate all even

DOI: 10.54254/2753-8818/2026.PU37671

permutations and form the backbone of blindfolded solving strategies. These algebraic insights not only explain the cube's combinatorial complexity but also illustrate broader principles in finite group theory, including group actions, generation, and representation theory. Future research may explore deeper connections between cube groups and other finite group invariants, extend representation-theoretic analyses to higher order cubes, or develop algorithmic optimizations inspired by the commutator-based approach. The Rubik's Cube thus remains a valuable pedagogical and research tool, bridging abstract algebra with practical computation and intuitive understanding.

References

[1] Rubik, E. (1981). *Rubik's cubic compendium*. Oxford University Press. (Original work published 1974)
[2] Weisstein, E. W. (2024). Rubik's cube. In *MathWorld–A Wolfram Web Resource*. Retrieved from https://mathworld.wolfram.com/RubiksCube.html
[3] Zassenhaus, H. (1982). Rubik's cube: A toy, a galois tool, group theory for everybody. *Physica A: Statistical Mechanics and its Applications, 114*, 629–637. DOI: 10.1016/0378-4371(82)90338-8
[4] Bagalá, N. (2017). *Semidirect products and Rubik's cube* (Master's thesis). University of Helsinki.
[5] Rokicki, T., Kociemba, H., Davidson, M., & Dethridge, J. (2013). The diameter of the Rubik's cube group is twenty. *SIAM Journal on Discrete Mathematics, 27*(2), 1082–1105. DOI: 10.1137/120894797
[6] Zuo, B., & Lai, H. (2023). From chaos to order: A group theory approach to the Rubik's cube. *ICACS 2023*, ACM. DOI: 10.1145/3631908.3631933
[7] Tan, Y. S. (2011). *On the diameter of Cayley graphs of finite groups* (REU Paper). University of Chicago.
[8] Daly, C., & Kingsnorth, J. (2025). The Rubik's cube and minimal representations of split group extensions. arXiv:2508.00687.
[9] Sun, T. (2024). Commutators in the Rubik's cube group. *The American Mathematical Monthly, 131*(1), 3–19. DOI: 10.1080/00029890.2023.2263158
[10] Montero, J. S. (2010). *Algorithm generation for Rubik's cube via group theory for blindfold cubing* (Bachelor's thesis). University of the Philippines Mindanao.