$n \times n \times n$ Rubik’s Cubes and God’s Number
A Group Theoretical Analysis

Daniel Salkinder

Abstract

The Rubik’s Cube is the most popular puzzle in the world. Two of its studied aspects are God’s Number, the minimum number of turns necessary to solve any state, and the first law of cubology, a solvability criterion. We modify previous statements of the first law of cubology for $n \times n \times n$ Rubik’s Cubes, and prove necessary and sufficient solvability conditions. We compute the order of the Rubik’s Cube group and the number of distinct configurations of the $n \times n \times n$ Rubik’s Cube. Finally, we derive a lower bound for God’s Number using the group theoretical results and a counting argument.

1 Introduction

The Rubik’s Cube is the most famous and best-selling puzzle of all time, challenging generations of solvers since its invention by Erno Rubik in 1974. The original design is a $3 \times 3 \times 3$ cube where every face can rotate around its center. To solve the cube, one must rotate the faces to rearrange the cube into its solved state: where all faces are monochromatic. In 1981, Peter Sebesteny invented an extension of the Rubik’s Cube to a $4 \times 4 \times 4$ cube where all slices could rotate. Only a couple of years later, a $5 \times 5 \times 5$ cube was created. Today, there are many variations of the Rubik’s Cube, and cubes up to $17 \times 17 \times 17$ are widely sold. Additionally, there are variants designed like other platonic solids (Pyraminx, Megaminx, etc.), cubes that rotate on axes different than those of the Rubik’s Cube (Skewb, Square One, etc.), and many more. This paper will focus on the $n \times n \times n$ Rubik’s Cube.

The Rubik’s Cube has garnered significant attention from throughout the scientific community. Many mathematicians have studied the cube, giving
group theoretical analyses and solutions for certain cases [2, 3, 15]. Another well-studied facet of the Rubik’s Cube is God’s Number: the minimum number of face turns needed to solve the puzzle from any position [13, 14, 9, 17, 6]. Additionally, the Rubik’s Cube can act as a physical model of chaotic behaviour, which has led to applications in cryptography [7, 16] as well as physics [4, 10, 11].

With many speed Rubik’s Cube solving competitions around the world, the puzzle begs the question, ”What is the minimum number of moves necessary to solve the cube from any configuration?” Such an optimal algorithm has been deemed impossible for humans to find, and hence has been labeled God’s Algorithm, with the number of moves in the worst case being labeled God’s Number. Computer scientists like Rokicki [14] have used symmetry and sheer computational power to determine that this number is 26 for the original Rubik’s Cube, but this approach requires too much time to be applicable to general cubes. Others like Demaine [5] have found the growth rate of God’s Number for $n \times n \times n$ cubes.

We aim to approach the problem of finding God’s Number from a group theoretical perspective. To employ such a strategy, we first need to be able to count the number of configurations of an $n \times n \times n$ Rubik’s Cube. We do so with a criterion for solving the question ”under which conditions is a (scrambled) cube solvable?”, the first law of cubology. First discussed by Bandelow [1] for the original Rubik’s Cube in 1982, the first law of cubology has been attempted to be generalized by Bonzio et al. [3] in 2018, but the result of that paper proves insufficient to generate only valid configurations.

The present work presents a modified first law of cubology for the $n \times n \times n$ Rubik’s Cube. This is then used to find the number of distinct valid configurations. Finally, a counting and pigeonhole principle argument establishes the lower bound of God’s Number as $\Omega(n^2/\log n)$, which is in accordance with [5], and is generalizable to find better coefficients.

The paper is structured as follows: Section 2 provides definitions and mathematical notations used throughout the paper. Section 3 discusses the $n \times n \times n$ Rubik’s Cube group. Subsections 3.1 and 3.2 prove the necessary and sufficient conditions of the first law of cubology by analysing chosen subgroups. Subsection 3.3 finds the order of the $n \times n \times n$ Rubik’s Cube group. Section 4 gives a lower bound for God’s Number. The conclusion suggests potential future research.
2 Definitions

The $n \times n \times n$ Rubik’s Cube is an extension of the original $3 \times 3 \times 3$ Rubik’s Cube. It takes the form of an $n \times n \times n$ cube made out of $1 \times 1 \times 1$ pieces, and each $n \times n \times 1$ slice is free to rotate around its center. As per standard convention, the $1 \times 1 \times 1$ cubes along the outside of a Rubik’s Cube are called cubies and the colored $1 \times 1$ faces of the cubies are called stickers. We proceed to categorize the cubies as shown in Figure 1:

![Cubie types for a 7 x 7 x 7 Rubik's Cube](image1.png) ![Cubie types for a 6 x 6 x 6 Rubik's Cube](image2.png)

Figure 1: Cubie types for odd and even $n$: Corners (Red), Single Edges (Grey), Coupled Edges (Green), Center Corners (Blue), Center Edges (Orange), and Fixed Centers (Dark Grey)

Cubies with 3 stickers are denoted corners, with 2 stickers edges, and with 1 sticker centers. Centers can be split into fixed centers (Dark Grey in Figure 1a), center corners (Blue in Figure 1), and center edges (Orange in Figure 1). Fixed centers are at the middle of their corresponding face and do not move when that face is rotated. We note that fixed centers only exist for odd cubes, as seen in Figure 1a but not Figure 1b. Center corners are along the diagonals connecting the corner cubies of their corresponding face, and all remaining center cubies are center edges. Edges can be categorized as single edges (Grey in Figure 1) and coupled edges (Green in Figure 1). Single edges are at the middle of their corresponding edges and are in the same slice as fixed centers. Single edges also only exist for odd cubes, as seen in Figure 1a but not Figure 1b. All remaining edges are called coupled due to the existence of two edges with the same sticker colors in each orbit of these
edges. This paper will refer to the permutations of stickers on one cubie as orientations of that cubie, and permutations of similar cubies permutations.

We can also notation all possible moves on an \( n \times n \times n \) Rubik’s Cube. Like on a \( 3 \times 3 \times 3 \) Rubik’s Cube, the capital letters \( F, B, R, L, U, D \) denote single clockwise 90° turns of the Front, Back, Right, Left, Up, and Down faces, respectively. We call these moves face turns. To label rotations of all possible slices, \( F_k, B_k, R_k, L_k, U_k, D_k, 1 \leq k \leq \left\lfloor \frac{n}{2} \right\rfloor \) denote single clockwise 90° rotations of the \( k \)th slice from the corresponding face, as shown in Figure 2. For convenience, we omit the 1 when writing \( F, B, R, L, U, D \). When \( k > 1 \), we call these moves internal slice rotations. Any sequence of these slice rotations is a valid move. \( m^{-1} \) denotes the inverse of the move \( m \) (a single counterclockwise 90° rotation for slice rotations \( m \)). \( m^2 \) denotes doing move \( m \) twice (a 180° rotation of the slice moved by \( m \) for slice rotations). We call the sequence of moves \( mm^{-1}n^{-1} \) a commutator, denoted \([m, n]\). Similarly, we call the sequence of moves \( mm^{-1}n \) a conjugate, denoted \([m : n]\).

\[
\begin{align*}
R & \quad R_2 \quad R_3 \\
L & \quad L_2 \quad L_3
\end{align*}
\]

Figure 2: Notation for slice rotations for a \( 7 \times 7 \times 7 \) Rubik’s Cube. Red marks the three slices corresponding to face R, and blue for face L.

For the following definitions, we proceed similarly to 3. The set of all valid moves of the \( n \times n \times n \) Rubik’s Cube clearly forms a group with the operation of composition (\( \cdot \)), which we denote \( M_n \). This group is generated by the slice rotations defined above. We see that a move \( m \in M_n \) results in
a permutation of the stickers of the cube. Since there are $6n^2$ stickers on an $n \times n \times n$ cube, we may define a group homomorphism

$$\varphi : \text{M}_n \rightarrow S_{6n^2}$$

which sends moves $m$ to permutations $\varphi(m) \in S_{6n^2}$ corresponding to the permutation of the stickers induced by $m$.

The symmetry group of the $n \times n \times n$ Rubik’s Cube, which comprises of all permutations of stickers caused by a sequence of valid moves, can then be formally defined as $G := \varphi(\text{M}_n)$. This can also be expressed as $\text{M}_n/\ker(\varphi)$, which is formed by all classes of moves that produce the same configuration of the Rubik’s Cube. For example, the moves $RL$ and $FB$ are different elements in $\text{M}_n$ but both map to $\text{id}_{S_{6n^2}}$ under $\varphi$, meaning they correspond to the same element in $G$.

Next, we consider two important subsets of $S_{6n^2}$. We call the subset of $S_{6n^2}$ corresponding to all permutations of stickers of the $n \times n \times n$ Rubik’s Cube that can be obtained by disassembling and reassembling the cubies in such a way that preserves orbits of cubie permutations (i.e., we allow swapping two cubies if and only if there is a valid sequence of moves that brings one cubie to the position of the other cubie) the *space of configurations* of the $n \times n \times n$ Rubik’s Cube, denoted $S_{\text{conf}}$. We observe that $S_{\text{conf}}$ can also be represented as the group generated by slice rotations, edge flips (which flip the two stickers on one edge cubie), and corner twists (which cycle the three stickers on one corner cubie). Clearly, $G \subset S_{\text{conf}}$. We call a configuration $s \in S_{\text{conf}}$ valid if it can be obtained from the solved state by slice rotations. We call the subset of $S_{6n^2}$ corresponding to all valid configurations that are physically distinct the *space of distinct valid configurations*, denoted $S_{\text{phys}}$.

### 3 The $n \times n \times n$ Symmetry Group

Let $G$ act on the left on $S_{\text{conf}}$:

$$G \times S_{\text{conf}} \rightarrow S_{\text{conf}}$$

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

\footnote{This definition slightly differs from its analogue in [3] for purposes of generalizability to $n \times n \times n$ and clarification of allowed permutations}
3.1 The subgroups of $S_{\text{conf}}$

In this section, we study the structure of $G$ by analysing the subgroups of $S_{\text{conf}}$. The significant subgroups of $S_{\text{conf}}$ discussed in this section are $C'$, which permutes and orients corner cubies, $E'_S$, which permutes and orients single edges, $E'_{C_i}$, which permutes and orients the orbit of coupled edges in slice $i$, $Z'_{C_i}$, which permutes the orbit of center corners in slice $i$, and $Z'_{E_{i,j}}$, which permutes the orbit of center edges in slices $i$ and $j$.

Theorem 1. $C' \cong S_8 \times Z^8_3$

Theorem 2. $E'_S \cong S_{12} \times Z^{12}_2$

Proof. First, we note that $C'$ is the same for all cubes and that $E'_S$ is the same for all odd cubes, since the only slice rotations that affect corners and single edges are outer face rotations.

We see that there are always 8 corners on any cube and 12 single edges on any odd cube, so we label permutations $\sigma \in S_8$ for corners and $\tau_s \in S_{12}$.

We proceed to define orientation for corners and center edges as shown in Figure 3. Orientation for a corner cubie is defined as $x_i \in Z_3$ where 0 is when the White/Yellow sticker of the cube lines up with the White/Yellow faces in the solved state (as seen in Figure 3a), orientation 1 is a clockwise cycle of the stickers of orientation 0, and orientation 2 is a clockwise cycle of the stickers of orientation 1. We express $(x_1, x_2, \ldots, x_8)$ as a vector $x \in Z^8_3$.

![Figure 3: Orientation definition for corner cubies and single edge cubies](image-url)
Orientation for a single edge cubie is defined as $z_i \in \mathbb{Z}_2$ where 0 is when the cubie matches the alternating pattern shown in Figure 3b such that the orientation of the single edge in the solved state is 0. We express $(z_1, z_2, \ldots, z_{12})$ as a vector $z \in \mathbb{Z}_{12}^{12}$.

Therefore, there is a bijection between $C'$ and pairs of permutations and orientation vectors $(\sigma, x)$, so $C' \cong S_8 \times \mathbb{Z}_3^8$. Similarly, there is a bijection between $E'_S$ and pairs of permutations and orientation vectors $(\tau, z)$, so $E'_S \cong S_{12} \times \mathbb{Z}_{12}^{12}$.

**Theorem 3.** $E'_C \cong S_{24} \times \mathbb{Z}_{24}^{24}$

*Proof.* We examine the orbit of one coupled edge cubie in slice $i$. We see that the cubie can be in one of 24 positions, so permutations for coupled edges can be labeled as $\tau_{c_i} \in S_{24}, 1 < i \leq \left\lfloor \frac{n}{2} \right\rfloor$. One such orbit can be represented by looking at coupled edges on the $4 \times 4 \times 4$ as shown in Figure 4.

A more interesting pattern emerges when we look at the orbit of the stickers on that cubie, as it does not reach all possible sticker locations on the orbit of the coupled edge cubie. Physically, this means that the orientation of coupled edges is fixed by their permutation. We define orientation for coupled edges by $y_{ik} \in \mathbb{Z}_2$, where 0 orientation is matching the pattern in Figure 4 such that the orientation of each coupled edge in the solved state is 0. Again, we express $(y_{i1}, y_{i2}, \ldots, y_{i24})$ as a vector $y_i \in \mathbb{Z}_{24}^{24}$.

Therefore, similarly to our proof for corners and single edges, we establish a bijection between $E'_C$ and the pair $(\tau_{c_i}, y_i)$, giving $E'_C \cong S_{24} \times \mathbb{Z}_{24}^{24}$. \qed

**Theorem 4.** $Z'_C \cong S_{24}$

![Figure 4: Positions with 0 orientation for one coupled edge of a 4 × 4 × 4 Rubik's Cube](image-url)
Theorem 5. $Z'_{E_{i,j}} \cong S_{24}$

Proof. We start by examining the orbits of one center cubie. Figure 5 shows center cubie orbits for a $7 \times 7 \times 7$ cube.

We clearly see that center corners can be in any of 24 positions, so we label permutations of the centers in slice $i \rho_{c_i} \in S_{24}$ for $1 < i \leq \left\lfloor \frac{n}{2} \right\rfloor$. Since center cubies only have one sticker, they do not have orientation, so clearly $Z'_{C_i} \cong S_{24}$.

We note that orbits for center edges are also of size 24 (e.g. Red and Blue orbits in Figure 5b never coincide). Labeling center edges provides more of a challenge, so label based on the slices $i$ and $j$ parallel to $U$ and $R$ respectively which contain the center edge in the orbit in the top left quadrant of the front face (i.e., in Figure 5b, the red orbit would be labeled (2, 3), blue (3, 2), green (2, 4), and orange (3, 4)). So, we can label permutations of center edges $\rho_{e_{i,j}} \in S_{24}, 1 < i \leq \left\lfloor \frac{n}{2} \right\rfloor, 1 < j \neq i \leq \left\lceil \frac{n}{2} \right\rceil$. This also clearly gives $Z'_{E_{i,j}} \cong S_{24}$.

(a) Orbits of center corners for a $7 \times 7 \times 7$ Rubiks’s Cube
(b) Orbits of center edges for a $7 \times 7 \times 7$ Rubiks’s Cube

Figure 5: Orbits of centers
Theorem 6. $S_{conf_{odd}} \cong C' \times E'_S \times E'^{(n-3)/2}_C \times Z'^{(n-3)/2}_E \times Z'^{(n-3)^2/4}_E$

Proof. $S_{conf}$ is defined as the set of all permutations of orbits and orientation changes. Therefore, we establish a bijection between $S_{conf}$ and the tuple $(\sigma, \tau, r, z, t, x, y, z)$, with all permutations and orientation vectors defined in the above proofs, $1 < i \leq \frac{n-1}{2}, 1 < j \neq i \leq \frac{n+1}{2}$. This tuple is equivalent to $(c, e, z, c, z, e, z)$, $c \in C', e \in E'_C, z \in Z'_{E_i}, z, e \in Z'_{E_i,j}$, so $S_{conf_{odd}} \cong C' \times E'_S \times E'_C \times Z'_{C_i} \times Z'_{E_i,j}$. Therefore, $S_{conf_{odd}} \cong C' \times E'_S \times E'^{(n-3)/2}_C \times Z'^{(n-3)/2}_E \times Z'^{(n-3)^2/4}_E$. 

Theorem 7. $S_{conf_{even}} \cong C' \times E'^{(n-2)/2}_C \times Z'^{(n-2)/2}_E \times Z'^{(n-2)(n-4)/4}_E$

Proof. Similarly to the proof of Theorem 6 we establish a bijection between $S_{conf}$ and $(c, e, z, c, z, e, z)$, $c \in C', e \in E'_C, z \in Z'_{C_i}, z, e \in Z'_{E_i,j}$, so $S_{conf_{even}} \cong C' \times E'_C \times Z'_{C_i} \times Z'_{E_i,j} \cong C' \times E'^{(n-2)/2}_C \times Z'^{(n-2)/2}_C \times Z'^{(n-2)(n-4)/4}_E$. 

Corollary 1. $|S_{conf_{odd}}| = 24! \cdot 3^8 \cdot 12! \cdot 2^{12(n-2)} \cdot (24!)^{(n-3)(n+1)/4}$

Corollary 2. $|S_{conf_{even}}| = 24! \cdot 3^8 \cdot 2^{12(n-2)} \cdot (24!)^{(n)(n-2)/4}$

We calculate $|S_{conf}|$ for some small $n$. For a $2 \times 2 \times 2$ Rubik’s Cube, we get $|S_{conf}| = 8! \cdot 3^8 = |C'|$, which makes sense since the Pocket Cube is just made of 8 corners. The $3 \times 3 \times 3$ gives $|S_{conf}| = 8! \cdot 3^8 \cdot 12! \cdot 2^{12} = |C' \times E'_S|$, which again makes sense since the original Rubik’s Cube has only 8 corners and 12 edges. For a $5 \times 5 \times 5$, we get $|S_{conf}| = 8! \cdot 3^8 \cdot 12! \cdot 2^{36} \cdot (24!)^3$.

We have shown that an element of $S_{conf}$ can be represented as the tuple $(\sigma, \tau, r, z, c, e, x, y, z)$. Now, we use such tuples to represent elements of $S_{conf}$. The solved state or initial configuration corresponds to $(id_{S_{12}}, id_{S_{24}}, id_{S_{24}}, id_{S_{24}}, id_{S_{24}}, 0, 0, 0)$.

We now state and prove the necessary condition of the first law of cubology for an $n \times n \times n$ Rubik’s Cube.\(^2\)

\(^2\)This is in accordance with equation (1) from [3].

\(^3\)This statement of the first law of cubology refines the incorrect statement in Theorem 20 of [3]. Condition 5 has been altered to match our definition of orientation in Theorem 3. More importantly, condition 2 has been updated to give a stricter restraint on center edges.
Theorem 8. Any valid configuration \((\sigma, \tau_s, \rho_{ci}, \rho_{ci,j}, x, y, z)\) of an odd \(n \times n \times n\) Rubik’s Cube must satisfy the conditions:

1. \(\text{sgn}(\sigma) = \text{sgn}(\tau_s) = \text{sgn}(\rho_{ci})\)
2. \(\text{sgn}(\rho_{ci,j}) = \text{sgn}(\sigma)\text{sgn}(\tau_i)\text{sgn}(\tau_j)\)
3. \(\sum_i x_i = 0\)
4. \(\sum_i z_i = 0\)
5. \(y_i = 0\)

Proof. We prove by checking that these conditions are invariant under the generators of \(M_n\). Since the solved state trivially satisfies all of these conditions, as any valid configurations are in the orbit of the solved state, this would show that all valid configurations satisfy these conditions.

1. Face turns consist of 4-cycles on corners, single edges, orbits of center corners, and orbits of coupled edges. Since this induces odd permutations on corners, single edges, and orbits of center corners, this preserves condition 1.

Internal slice rotations consist of 4-cycles on orbits of coupled edges and center edges, two 4-cycles on orbits of center corners, and act as the identity permutation on corners and single edges. Since this induces even permutations on corners, single edges, and orbits of center corners, this also preserves condition 1.

Therefore, \(\text{sgn}(\sigma) = \text{sgn}(\tau_s) = \text{sgn}(\rho_{ci})\).

2. Face turns induce odd permutations on corners and any orbit of center edges and induce even permutations on any orbits of coupled edges. So, \(\text{sgn}(\rho_{ci,j}) = \text{sgn}(\sigma)\text{sgn}(\tau_i)\text{sgn}(\tau_j)\) holds under face turns.

Rotations of internal slice \(i\) act as the identity on corners, induce odd permutations of coupled edges in orbit \(i\) and also induce odd permutations on orbits of center edges \(i, j\) or \(j, i\). Therefore, \(\text{sgn}(\rho_{ci,j}) = \text{sgn}(\sigma)\text{sgn}(\tau_i)\text{sgn}(\tau_j)\) is preserved for each slice \(i\) under internal slice rotations.

3. Internal slice rotations act as the identity on corners, so we only consider the effects of face turns. By our definition of corner orientation in Theorem III turning the white or yellow face does not change the
orientation of any corners, and turning any other face increase two corner orientations by 1 and decreases two corner orientations by 1, which shows $\sum_i x_i = 0$.

4. Internal slice rotations also act as the identity on single edges, so we again only consider the effects of face turns. By our definition of corner orientation in Theorem 2 any face turn changes the orientation of all 4 single edges on that face, which preserves $\sum_i z_i = 0$.

5. By the definition of orientation for coupled edges in Theorem 3 the orientation of any coupled edge never changes due to it being fixed by the orbits of its stickers.

\[ \text{Theorem 9. Any valid configuration } (\sigma, \tau_{c_i}, \rho_{c_i}, \rho_{e_{i,j}}, x, y_i, z) \text{ of an even } n \times n \text{ Rubik’s Cube must satisfy the conditions:} \]

\begin{enumerate}
  \item $\text{sgn}(\sigma) = \text{sgn}(\rho_{c_i})$
  \item $\text{sgn}(\rho_{e_{i,j}}) = \text{sgn}(\sigma) \text{sgn}(\tau_i) \text{sgn}(\tau_j)$
  \item $\sum_i x_i = 0$
  \item $y_i = 0$
\end{enumerate}

\textit{Proof.} We proceed as for Theorem 8 and prove by checking that these conditions are invariant under the face turns and internal slice rotations

1. Face turns induce odd permutations on corners and any orbit of center corners, which preserves condition 1. Internal slice rotation act as the identity on corners and induce even permutations of the orbit of center corners in their slice, so condition 1 holds.

2. Fact turns act as odd permutations on corners and center edges and as odd permutations on coupled edges, which preserved condition 2. Internal slice rotations induce odd permutations of center edges in their slice and coupled edges in their slice, while acting as the identity on other coupled edges and corners, which also preserves condition 2.

3. This is equivalent to Condition 3 of Theorem 8

4. This is equivalent to Condition 5 of Theorem 8

\[ \square \]
3.2 The subgroups of G

In this section, we continue to study the structure of $G$ by analyzing some important commuting subgroups. For these subgroups, we again use a construction analogous to that of $[3]$. Namely, the first subgroups discussed in this section are $C$, which permutes only corners, preserves orientation, and acts as the identity on all other cubies, $E_S$, which permutes only single edges, $E_{C_i}$, which permutes only coupled edges in slice $i$, $Z_{C_i}$, which permutes only center corners in slice $i$, and $Z_{E_{i,j}}$, which permutes only center edges in slice $i,j$. For each subgroup, we consider odd and even cubes separately. Then, we discuss the subgroups $O_C$ and $O_E$ which orient only corners and single edges respectively and preserve permutation.

**Theorem 10.** $C_{odd} \cong C_{even} \cong A_8$

**Proof.** We start as in our proof of Theorem 4 by noting that $C$ is the same for any size Rubik’s Cube.

First, we show $A_8 \subseteq C$. We see that the move

$$ m_c = [[R : U], D] = (RUR^{-1})D(RU^{-1}R^{-1})D^{-1} $$

is a 3-cycle on corners for a $3 \times 3 \times 3$ Rubik’s Cube (as shown in Figure 6a) and for any $n \times n \times n$ Rubik’s Cube. Since all the corners are in the same orbit, for any there exists an element $g \in G$ that brings it to one of the cubies permuted by $m_c$, so $g \cdot m_c \cdot g^{-1}$ gives 3-cycles containing any corners, which suffice to generate $A_8$.

Since there are 8 corners, clearly $C \subseteq S_8$. By condition 1 of Theorem 8 and condition 1 of Theorem 9, a permutation of corners that does not permute center corners must be even for both odd and even cubes, so $C \subseteq A_8$, which gives $C_{odd} \cong C_{even} \cong A_8$.

![3-cycles for corners and single edges](image)

(a) $m_c = [[R : U], D]$  (b) $m_{es} = [F, [R : S]]$  (c) $m'_{es} = U^2D^2F^2U^2D^2B^2$

Figure 6: 3-cycles for corners and single edges
Theorem 11. \( E_S \cong A_{12} \)

\textit{Proof.} We proceed as we did for Theorem 10. First, we show \( A_{12} \leq E_S \). We want to create a move that permutes elements in \( E_S \).

This is simplified if we allow slice rotations of the central slice. We can reconcile the issue of centers being fixed in our definition of the cube by considering such a move as a combination of all parallel slice rotations and then a shift in notation for following moves. As such, we denote the move \( M \) as the rotation of the central slice between \( L \) and \( R \), \( E \) between \( U \) and \( D \), and \( S \) between \( F \) and \( B \). Figure 6c shows a move equivalent to \( M_2 B_2 M_2 B_2 \).

We see that the move 

\[ m_e = [F, [R : S]] \]

is a 3-cycle on single edges for a 3 \( \times \) 3 \( \times \) 3 Rubik’s Cube (as shown in Figure 6b) that holds for any \( n \times n \times n \) Rubik’s Cube. Since all 12 single edges are in the same orbit, for any there exists an element \( g \in G \) that brings it to one of the cubies permuted by \( m_e \), so \( g \cdot m_e \cdot g^{-1} \) gives 3-cycles containing any single edges, which suffice to generate \( A_{12} \).

Since there are 12 single edges, clearly \( E_S \leq S_{12} \). By condition 1 of Theorem 8, a permutation of single edges that does not permute corners must be even, so \( E_S \leq A_{12} \), which gives \( E_S \cong A_{12} \). \( \square \)

Theorem 12. \( Z_{C_{i,odd}} \cong Z_{C_{i,even}} \cong A_{24} \)

Theorem 13. \( Z_{E_{i,j,odd}} \cong Z_{E_{i,j,even}} \cong A_{24} \)

\textit{Proof.} We proceed as we did for Theorem 10. First, we show \( A_{24} \leq Z_{C_{i}} \) and \( A_{24} \leq Z_{E_{i,j}} \). We see that the move 

\[ m_{zc} = [[R_2^{-1}, D_2], F^{-1}] \]

is a 3-cycle on center corners in the second slice of an \( n \times n \times n \) Rubik’s Cube, as shown in Figure 7a. We generalize this to move 

\[ m_{zi,j} = [[R_j^{-1}, D_i], F^{-1}] \]

which gives a 3-cycle on centers in slice \( i \) of an \( n \times n \times n \) Rubik’s Cube. We note that when \( i = j \), this is a 3-cycle on center corners and when \( i \neq j \) on center edges, as shown in Figure 7b. Also, we substitute \( M \) for \( R_{n+1} \) to
give a 3-cycle on center edges whose orbit is in the central slice\(^4\). Again, by
a move \(g \cdot m_{zi,j} \cdot g^{-1}\), we 3-cycle centers in the same orbit, giving \(A_{24} \leq Z_{C_i}\)
and \(A_{24} \leq Z_{E_{i,j}}\).

Since there are 24 centers in any orbit, clearly \(Z_{C_i} \leq S_{24}\) and \(Z_{E_{i,j}} \leq S_{24}\).

By condition 1 of Theorem 8 and condition 1 of Theorem 9, a permutation

of center corners that does not permute corners must be even, so \(Z_{C_i} \leq A_{24}\),
which gives \(Z_{C_i, odd} \cong Z_{C_i, even} \cong A_{24}\).

By condition 2 of Theorem 8 and condition 2 of Theorem 9, a permutation

of center edges that does not permute corners or coupled edges must be even,
which means \(Z_{E_{i,j}} \leq A_{24}\), so \(Z_{E_{i,j}}^{odd} \cong Z_{E_{i,j}}^{even} \cong A_{24}\).

\[\square\]

**Theorem 14.** \(E_{C_i}^{odd} \cong A_{24}\), \(E_{C_i}^{even} \cong S_{24}\)

**Proof.** Once again, we first show \(A_{24} \leq E_{C_i}\). We see that the move

\[m_{ec_2} = [[F^{-1}, U], D_2]\]  \hspace{1cm} (5)

is a 3-cycle on coupled edges in the second slice of an \(n \times n \times n\) Rubik’s Cube, as shown in Figure 7a. We generalize this to move

\[m_{ec_i} = [[F^{-1}, U], D_i]\]  \hspace{1cm} (6)

\[\text{This move with center slice turns can serve as a replacement for the incorrect move}\ w\ \text{on the } 5 \times 5 \times 5\ \text{Rubik’s Cube in Theorem 13 of [3], which permuted center corners instead of center edges}\]

\[\text{This corrects the subgroup of center edges for a } 6 \times 6 \times 6\ \text{Rubik’s Cube from Theorem 17 of [3].}\]
which gives a 3-cycle on centers in slice $i$ of an $n \times n \times n$ Rubik’s Cube. By a move $g \cdot m_{ce} \cdot g^{-1}$, we 3-cycle coupled edges in the same orbit, giving $A_{24} \leq E_{C_i}$.

Since there are 24 coupled edges in any orbit, clearly $E_{C_i} \leq S_{24}$.

For odd cubes, by condition 2 of Theorem 8, a permutation of coupled edges that does not permute corners or center edges must be even, so $E_{C_i, odd} \leq A_{24}$, which gives $E_{C_i, odd} \cong A_{24}$.

For even cubes, we can find a move that induces an odd permutation of center edges. For a $4 \times 4 \times 4$ or $5 \times 5 \times 5$ Rubik’s Cube, one such move is $m = (R^2R_2^2B^2,U^2L_2U^2R_2^{-1}U^2R_2U^2F^2R_2F^2L_2^{-1})$ (shown in Figure 8b), which can be generalized to create an odd permutation for orbit $i$ of an $n \times n \times n$ Rubik’s Cube by substituting $R^2R_2^2 \ldots R_i^2$ for $R^2R_2^2$, $R_i$ for $R_2$, and $L_i$ for $L_2$ and then combining such moves. Therefore, from this odd permutation and $A_{24}$, we can generate all odd permutations, so $E_{C_i, even} \cong S_{24}$.

\[ \text{Theorem 15. } O_C \cong \mathbb{Z}_3^7 \]

\[ \text{Proof. First, we show } \mathbb{Z}_3^7 \leq O_C \] We see that the move

\[ m_o = [(F,L)^2,U] \] (7)

changes the orientation of 2 corners for any $n \times n \times n$ Rubik’s Cube, as shown in Figure 9a. Again, for some $g \in G$, $g \cdot m_o \cdot g^{-1}$ can change the orientation of 2 corners mod 3, which generates $\mathbb{Z}_3^7$.

Since there are 8 corners, clearly $O_C \leq \mathbb{Z}_3^8$. By condition 3 of Theorem 8 and Theorem 9 $O_C < \mathbb{Z}_3^3$, so $\mathbb{Z}_3^3 \leq O_C$. \[ \square \]
Theorem 16. \( O_E \cong \mathbb{Z}_2^{11} \)

**Proof.** We show \( \mathbb{Z}_2^{11} \leq O_C \) We see that the move

\[
m_{oc} = [F E F^2 E^2 F, U]
\]

changes the orientation of 2 single edges, as shown in Figure 9b. For some \( g \in G \), \( g \cdot m_{oc} \cdot g^{-1} \) can change the orientation of 2 single edges \( \mod 2 \), which generates \( \mathbb{Z}_2^{11} \).

Since there are 12 corners, clearly \( O_C \leq \mathbb{Z}_2^{11} \). By condition 4 of Theorem 8, \( O_C \leq \mathbb{Z}_2^{12} \), so \( O_C \cong \mathbb{Z}_2^{11} \). \( \square \)

Now, we can prove the sufficient condition of the first law of cubology:

**Theorem 17.** Any configuration \((\sigma, \tau_s, \tau_{c_i}, \rho_{c_i}, \rho_{e_{i,j}}, x, y_i, z)\) of an odd \( n \times n \times n \) is valid if:

1. \( \text{sgn}(\sigma) = \text{sgn}(\tau_s) = \text{sgn}(\rho_{c_i}) \)
2. \( \text{sgn}(\rho_{e_{i,j}}) = \text{sgn}(\sigma) \text{sgn}(\tau_i) \text{sgn}(\tau_j) \)
3. \( \sum_i x_i = 0 \)
4. \( \sum_i z_i = 0 \)
5. \( y_i = 0 \)

**Proof.** We by prove by showing there exists a sequence of moves that brings a configuration \((\sigma, \tau_s, \tau_{c_i}, \rho_{c_i}, \rho_{e_{i,j}}, x, y_i, z)\) satisfying the above conditions to the solved state, \((\text{id}_{S_8}, \text{id}_{S_{12}}, \text{id}_{S_{24}i}, \text{id}_{S_{24}i}, \text{id}_{S_{24}i,j}, 0, 0, 0)\).

First, we undergo a series of moves that will make all our permutations even. If \( \text{sgn}(\sigma) = -1 \), we do \( F \). Now, we know \( \text{sgn}(\sigma) = \text{sgn}(\tau_s) = \)
sgn(ρ_{ci}) = +1. If sgn(τ_i) = −1, we do F_i. Now, we know sgn(ρ_{ei,i}) = sgn(σ)sgn(τ_i)sgn(τ_j) = +1. We call this move sequence e. We let

\[ e \cdot (σ, τ_s, τ_{c_1}, ρ_{c_1}, ρ_{ei,i}, x, y_i, z) = (σ', τ_s', τ_{c_{i_1}}, ρ_{c_{i_1}}, ρ_{ei,i}, x', y_i', z') \]

Next, we get the permutations to the solved state. By Theorem 10, there exists a move \( p_c \in C \) such that

\[ p_c \cdot (σ', τ_s', τ_{c_1}, ρ_{c_1}, ρ_{ei,i}, x', y_i', z') = (id_{S_8}, τ', ρ_{c_1}', ρ_{ei,i}', x', y_i', z') \]

Similarly, by Theorems 11 and 12 there exist moves \( p_{e_{ci}} \in E_{S} \), and \( p_{z_{ei}} \in Z_{C_i} \) such that

\[ p_{e_{ci}} \cdot p_{e_i} \cdot (id_{S_8}, τ_{c_{i_1}}, ρ_{c_{i_1}}', ρ_{ei,i}', x', y_i', z') = (id_{S_8}, id_{S_{12}}, τ_{c_{i_1}}', id_{S_8}, ρ_{ei,i}', x', y_i', z') \]

And, by Theorems 13 and 14 there exist moves \( p_{e_{ci}} \in E_{C_i} \), and \( p_{z_{ei,i}} \in Z_{E_{c_i}} \) such that

\[ p_{e_{ci}} \cdot p_{e_i} \cdot (id_{S_8}, id_{S_{12}}, τ_{c_{i_1}}', id_{S_8}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_{24}}, i, x', y_i', z') = (id_{S_8}, id_{S_{12}}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_{24}}, i, x', y_i', z') \]

Then, we can deal with orientation. By condition 5 of Theorem 8, \( y_i' = 0 \).

By Theorems 13 and 16 and conditions 3 and 4 of 8 there exist moves \( o_c \in O_C \) and \( o_e \in O_E \) such that

\[ o_c \cdot o_e \cdot p_{e_{ci}} \cdot (id_{S_8}, id_{S_{12}}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_{24}}, i, x', y_i', z') = (id_{S_8}, id_{S_{12}}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_8}, id_{S_{24}}, i, 0, 0, 0) \]

Therefore, the move \( m = ep_c p_{e_{ci}} p_{e_i} p_{z_{ei}} o_c o_e \in G \) brings any configuration that satisfies the above conditions to the solved state, meaning any configuration that satisfies the conditions is valid because it can be reached from the solved state by move \( m^{-1} \).

**Theorem 18.** Any configuration \((σ, τ_{c_1}, ρ_{c_1}, ρ_{ei,i}, x, y_i, z)\) of an even \( n \times n \times n \) is valid if:

1. \( sgn(σ) = sgn(ρ_{ci}) \)
2. \( sgn(ρ_{ei,i}) = sgn(σ)sgn(τ_i)sgn(τ_j) \)
3. \( \sum_i x_i = 0 \)
4. \( y_i = 0 \)

**Proof.** By similar logic to the proof of Theorem 18 there exist moves \( e, p_c \in C, p_{z_{ei}} \in Z_{C_i}, p_{e_{ci}} \in E_{C_i}, p_{z_{ei,i}} \in Z_{E_{c_i}}, o_c \in O_C, \) and \( o_e \in O_E \) such that \( m = ep_c p_{e_{ci}} p_{e_i} p_{z_{ei}} o_c o_e \in G \) brings any configuration that satisfies the above conditions to the solved state, meaning any such configuration is valid.
3.3 The order of G

We note the action of G on $S_{\text{conf}}$ is free, i.e. $\forall s \in S_{\text{conf}}, g \cdot s = s \Rightarrow g = \text{id}_G$ and hence all stabilizers $G_s = g \in G : g \cdot s = s$ are clearly trivial. Therefore, there is also a bijection between any orbit $\mathcal{O} = G \cdot s = g \cdot s | g \in G$ and $G$. Therefore, by the orbit counting theorem (or the Cauchy-Frobenius-Burnside lemma), the number of orbits $|S_{\text{conf}} \setminus G|$ is

$$|S_{\text{conf}} \setminus G| = \frac{1}{|G|} \sum_{s \in S_{\text{conf}}} |G_s| = \frac{|S_{\text{conf}}|}{|G|}$$

So, we can find the order of group $G$ by counting the number of orbits in $S_{\text{conf}}$. We can count by analysing the formulations of the law of cubology with different initial configurations.

First, we count the number of orbits for odd cubes. For the first condition, we can assign $+1$ or $-1$ to each of $\text{sgn} (\sigma), \text{sgn} (\tau)_s$, and $\text{sgn} (\rho_{c_i})$, which will only be in the same orbit if all signs are flipped, giving $2^{2 + \frac{n-3}{2}}/2 = 2^{\frac{n+1}{2}}$ choices. For the second condition, we have choices $\text{sgn} (\rho_{e_{i,j}}) = \pm \text{sgn} (\sigma) \text{sgn} (\tau_i) \text{sgn} (\tau_j)$ for each center edge, giving $2^{\frac{(n-3)^2}{4}}$ choices. For condition 3, we can have $\sum_i x_i = 0, 1,$ or $2$, giving $3$ choices. Similarly, condition 4 gives $2$ choices. We can choose any starting $y_i$, which we recall is a vector containing coupled edge orientations in orbit $i$, giving us $2^{24 \frac{n-3}{2}}$ choices. So, $|S_{\text{conf}} \setminus G| = 2^{\frac{(n-9)^2 + n+1}{2}} \cdot 3 \cdot 2^{12(n-3)}$.

For even cubes, the first condition gives $2^{\frac{n+2}{2}}$ choices. The second condition gives $2^{\frac{(n-2)^2}{4}}$, the third, and the last $2^{12(n-2)}$. Therefore, $|S_{\text{conf}} \setminus G| = 2^{\frac{(n-2)^2}{4}} \cdot 3 \cdot 2^{12(n-2)}$.

**Corollary 3.** $|G|_{\text{odd}} = 8! \cdot 3^7 \cdot 12! \cdot 2^{11} \cdot (24!)^{\frac{(n-3)(n+1)}{4}} / 2^{(\frac{n-3}{2})^2 + (\frac{n-3}{2}) + 1}$

**Corollary 4.** $|G|_{\text{even}} = 8! \cdot 3^7 \cdot (24!)^{\frac{(n)(n-2)}{4}} / 2^{(\frac{n-2}{2})^2}$

We can compute some values to compare against established results. For the $2 \times 2 \times 2$, we get $|G| = 8! \cdot 3^7$, which is equal to $|C| \cdot |O_C|$. For the $3 \times 3 \times 3$ Rubik’s Cube, $|G| = 8! \cdot 3^7 \cdot 12! \cdot 2^{11}$, which gives the well known $43\text{quintillion}$ valid configurations. For the $5 \times 5 \times 5$, we get $|G| = 8! \cdot 3^7 \cdot 12! \cdot 2^{8 \cdot (24)!}$

For all $2 \leq n \leq 9$, this formula matches the output of a self-made GAP program that generates and finds the order of the symmetry group of the $n \times n \times n$ Rubik’s Cube (the program takes too long to be viable for larger $n$).\footnote{Once again, this rectifies the incorrect order for $G_5$ in [3].}
4 God’s Number

We recall that God’s Number is defined as the minimum number of face
turns needed to solve the puzzle from any position. It has been shown to be 26
for the original Rubik’s Cube (we use the quarter turn metric). This section
derives a lower bound for God’s Number by considering the least number of
moves necessary to reach at least the number of physically distinct positions.
So, we want to calculate the size of $S_{phys}$.

We let $G$ act on the left on $S_{phys}$:

$$G \times S_{phys} \rightarrow S_{phys}$$

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

By the Cauchy-Frobenius-Burnside lemma,

$$|S_{phys} \setminus G| = \frac{1}{|G|} \sum_{s \in S_{phys}} |G_s|$$

Since $S_{phys} \subset G$, $|S_{phys} \setminus G| = 1$, since for every pair $s_1, s_2 \in S_{phys}$, there
exists $g \in G$ such that $g \cdot s_1 = s_2$.

**Theorem 19.** $|G_s|_{odd} = \left(\frac{24^n}{2}\right)^{\frac{(n-3)(n-1)}{4}}$, $|G_s|_{even} = \left(\frac{24^n}{2}\right)^{\frac{(n-2)^2}{4}}$

$G_s$ is the stabilizer of $s$ in $G$, so to count $|G_s|$, we must determine how
many elements $g \in G$ do not change the physical appearance of the cube,
thus all mapping to the same physically distinct configuration. Clearly, any
permutation or orientation change of corners or edges produces a physically
distinct configuration, so we only count valid permutations of centers that
appear the same.

For any orbit of centers, permutations of the 4 centers on each face result
in physically identical valid configurations. We also recall that by conditions
1 and 2 of Theorems 8 and 9 a permutation within an orbit of center cor-
ners or center edges that does not permute corners or edges must be even.
Therefore, we get $4!^6/2$ such permutations for each orbit. The result clearly
follows from the number of orbits of centers for odd and even cubes.
Corollary 5. \( |S_{\text{phys}}|_{\text{odd}} = 8! \cdot 3^7 \cdot 12! \cdot 2^{10} \cdot \frac{(n-3)(n+1)}{4} \cdot \frac{(24)^n}{(24)^6} \cdot \frac{(n-9)(n-1)}{4} \)

Corollary 6. \( |S_{\text{phys}}|_{\text{even}} = 8! \cdot 3^7 \cdot \frac{(24)!}{(24)^6} \cdot \frac{(n)(n-2)}{4} \cdot \frac{(n-2)^2}{4} \)

Theorem 20. God’s Number grows as \( \Omega\left(\frac{n^2}{\log n}\right) \)

Proof. We have 3\( n \) slices (counting center slices for odd cubes) for an \( n \times n \times n \) Rubik’s Cube, which means we have 6\( n \) basic moves. After \( k \) moves, the cube can achieve at most \( (6n)^k \) configurations. By the pigeonhole principle, if any valid configuration can be solved in \( k \) basic moves, the \( \sum (6n)^k \) configurations reached in \( k \) moves must be more than the number of distinct valid configurations. Therefore, for even cubes,

\[
8! \cdot 3^7 \cdot \frac{(n)(n-2)}{4} \cdot \frac{(n-2)^2}{4} \leq \sum (6n)^k \leq (6n)^{k+1}
\]

\[
(k + 1) \log 6n \geq \frac{(n)(n-2)}{4} \log 24! - \frac{(n-2)^2}{4} \log 24^6
\]

\[
k \geq \frac{(n)(n-2)}{4} \log 24! - \frac{(n-2)^2}{4} \log 24^6
\]

\[
\log 6n
\]

We note that this argument can be tuned by finding the number of sequences of \( k \) moves that give distinct configurations (for example, omitting all instances of \( mm^{-1} \) or \( m^3 \)) to give a better coefficient for the lower bound.

5 Conclusion

We have modified and proven the law of cubology, which gives a necessary and sufficient solvability criterion for the \( n \times n \times n \) Rubik’s Cube. We derived the order of the Rubik’s Cube group and number of distinct valid configurations for any size cube. We were able to determine an \( \Omega\left(\frac{n^2}{\log n}\right) \) lower bound for God’s Number.

These results can be applied to cryptography and physics by quantifying the number of states when the randomized Rubik’s Cube is used as a physical model for chaos.

However, there are still many more pertinent questions in this field. The following are a few suggestions:
In addition to God’s Number, The Devil’s Number examines the shortest length of an algorithm that passes every possible state. An analysis of the diameter of the Rubik’s Cube group could provide a lower bound for this less widely studied quantity.

Randomization of a Rubik’s Cube is a fascinating topic. God’s Number could be applied to determine the optimal number of turns to make to scramble a cube.

The Rubik’s Cube can be further generalized to other shapes, and even more dimensions. A group theoretical approach can give the number of configurations of such constructions.
References

[1] C. Bandelow. *Inside Rubik’s cube and beyond.* Birkhauser, 1982.

[2] S. Bonzio, A. Loi, and L. Peruzzi. The first law of cubology for the rubik’s revenge. *Mathematica Slovaca*, 67(3):561–572, 2017.

[3] S. Bonzio, A. Loi, and L. Peruzzi. On the $n \times n \times n$ rubik’s cube. *Mathematica Slovaca*, 68(5):957–974, Oct 2018.

[4] B. Czech, K. Larjo, and M. Rozali. Black holes as rubik’s cubes. *Journal of High Energy Physics*, 2011(8), 2011.

[5] E. D. Demaine, M. L. Demaine, S. Eisenstat, A. Lubiw, and A. Winslow. Algorithms for solving rubik’s cubes. *Algorithms – ESA 2011*, page 689–700, 2011.

[6] E. D. Demaine, S. Eisenstat, and M. Rudoy. Solving the rubik’s cube optimally is np-complete. *CoRR*, abs/1706.06708, 2017.

[7] A.-V. Diaconu and K. Loukhaoukha. An improved secure image encryption algorithm based on rubik’s cube principle and digital chaotic cipher. *Mathematical Problems in Engineering*, 2013:1–10, 2013.

[8] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.

[9] D. Kunkle and G. Cooperman. Twenty-six moves suffice for rubik’s cube. *Proceedings of the 2007 international symposium on Symbolic and algebraic computation - ISSAC ’07*, 2007.

[10] X. Lai, Z. Shi, Z. Pu, P. Zhang, X. Zhang, H. Yu, and D. Li. A rubik’s microfluidic cube. *Microsystems & Nanoengineering*, 6(1), 2020.

[11] C. L. Lee and M. C. Huang. The rubik’s cube problem revisited: A statistical thermodynamic approach. *The European Physical Journal B*, 64(2):257–261, 2008.

[12] The mathematics of the rubik’s cube, February 2010.

[13] T. Rokicki. Towards god’s number for rubik’s cube in the quarter-turn metric. *The College Mathematics Journal*, 45(4):242–253, 2014.
[14] T. Rokicki, H. Kociemba, M. Davidson, and J. Dethridge. The diameter of the rubik’s cube group is twenty. *SIAM Review*, 56(4):645–670, 2014.

[15] M. D. Sikirić. A variation on the rubik’s cube, 2020.

[16] E. Volte, J. Patarin, and V. Nachef. Zero knowledge with rubik’s cubes and non-abelian groups. *Cryptology and Network Security*, page 74–91, 2013.

[17] J. Weed. Sub-optimal multi-phase path planning: A method for solving rubik’s revenge, 2016.