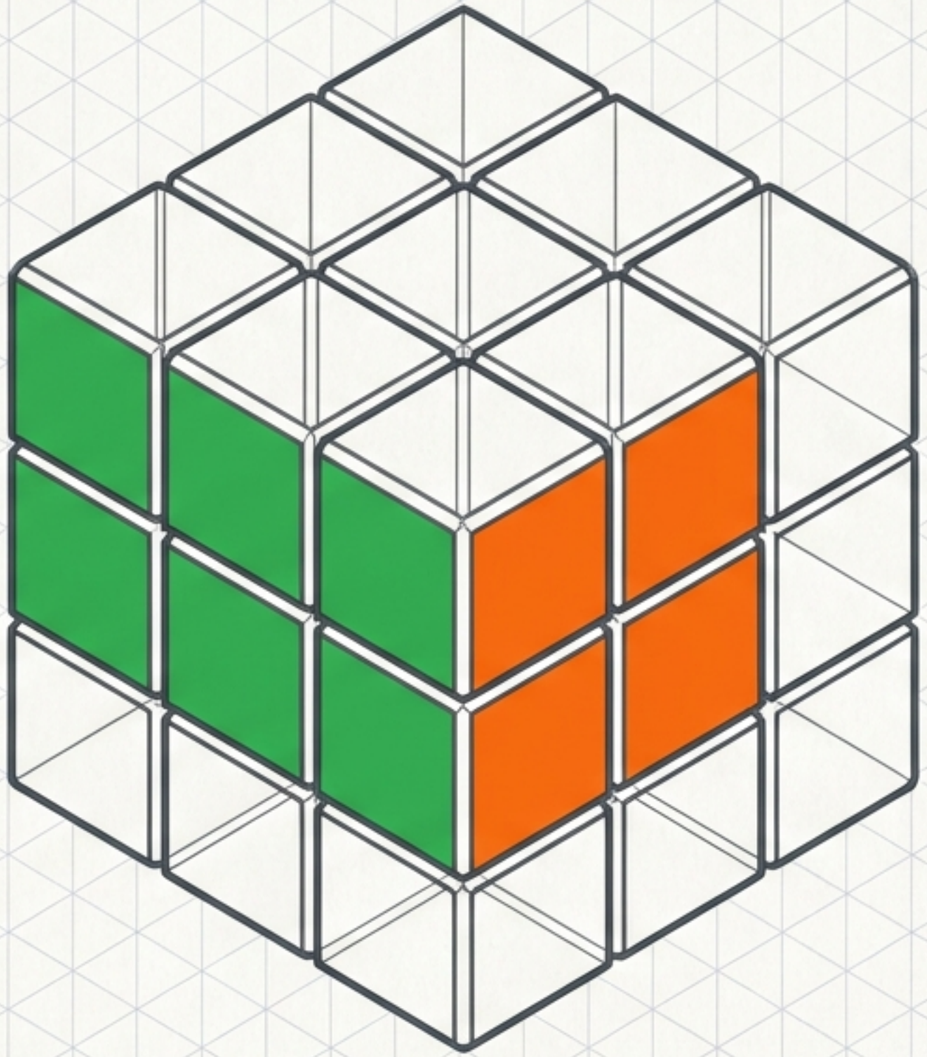
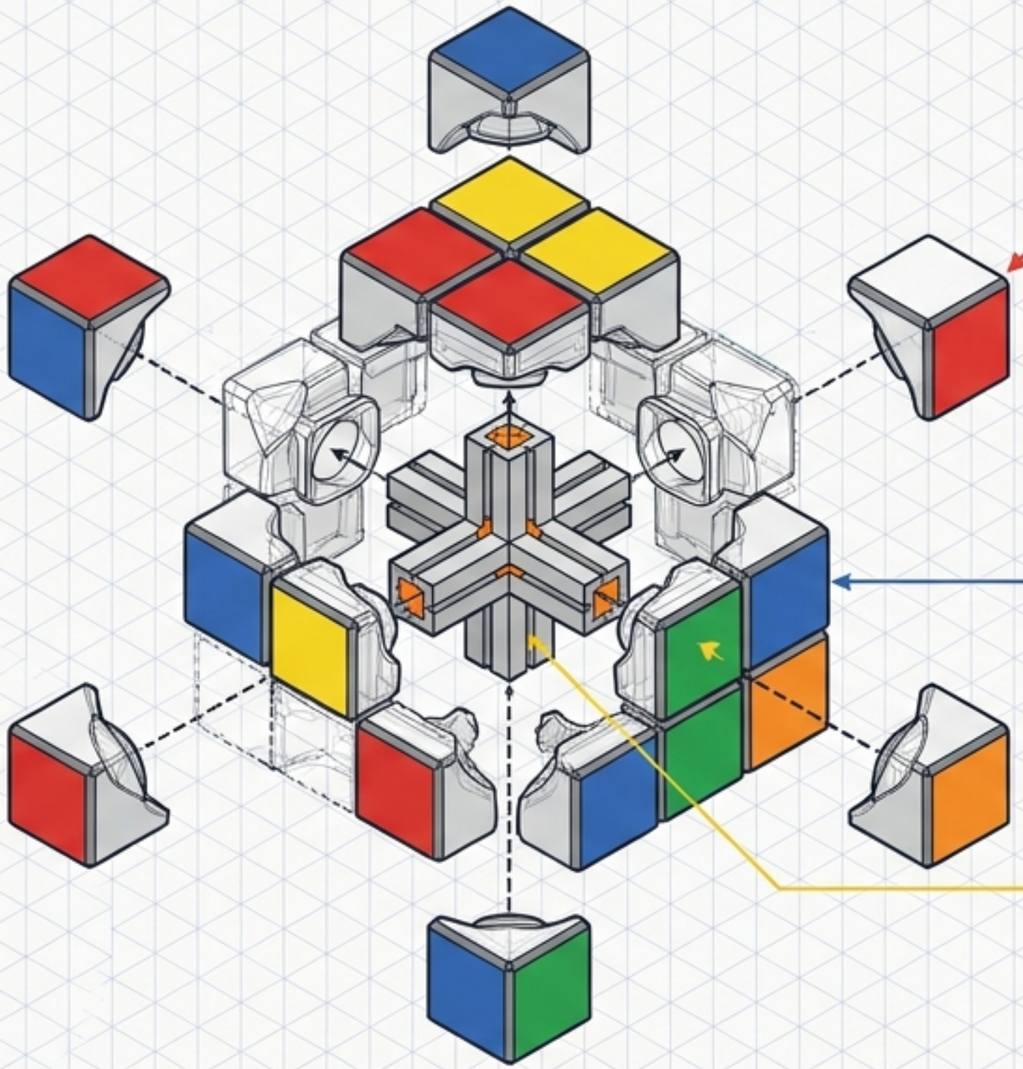
God's Number: The Math Behind the Rubik's Cube

A scrambled cube. 43 quintillion states. And the group theory that proves 20 moves is always enough.



Authored by Ayush Subedi



Corners: 8 pieces x 3 orientations.

Constraint: Total twist must equal 0 (mod 3).

Formula: $(8! \times 3^8) / 3$

Edges: 12 pieces x 2 orientations.

Constraint: Parity of corner and edge permutations must match.

Formula: $(12! \times 2^{12}) / 4$

Centers: **6 fixed** pieces, defining the face colors.

$$|G_{RC}| = 43,252,003,274,489,856,000 \text{ (roughly } 4.3 \times 10^{19})$$

G_{RC} is a proper subgroup of S_{48}. Most physical permutations of the 48 moving stickers are physically unreachable by legal moves.

A **group** strips away everything except the bare minimum structure needed to capture symmetry and reversibility.

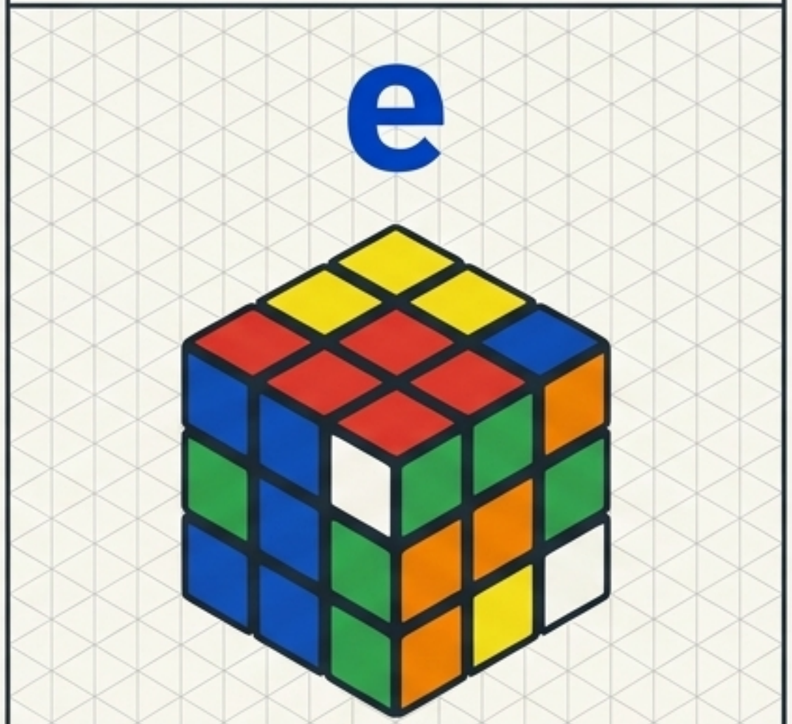
Group Theory Diagnostic Matrix

	Integers under Addition ($\mathbb{Z}$, +)	Positive Reals under Subtraction ($\mathbb{R}>0$, −)	2x2 Real Matrices under Multiplication ($M2(\mathbb{R})$, x)	The Rubik's Cube (G_{RC})
Closure (Combining elements stays inside)	✓	✗ 3 − 5 = −2 (Fails)	✓	✓
Associativity (Grouping doesn't matter)	✓		✓	✓
Identity (A "do nothing" element exists)	✓ e=0		✓	✓
Inverses (Every action can be undone)	✓ e=−n		✗ Singular matrices have no inverse	✓

Closure

Any sequence of standard moves (M) produces another valid, reachable cube state.

Identity

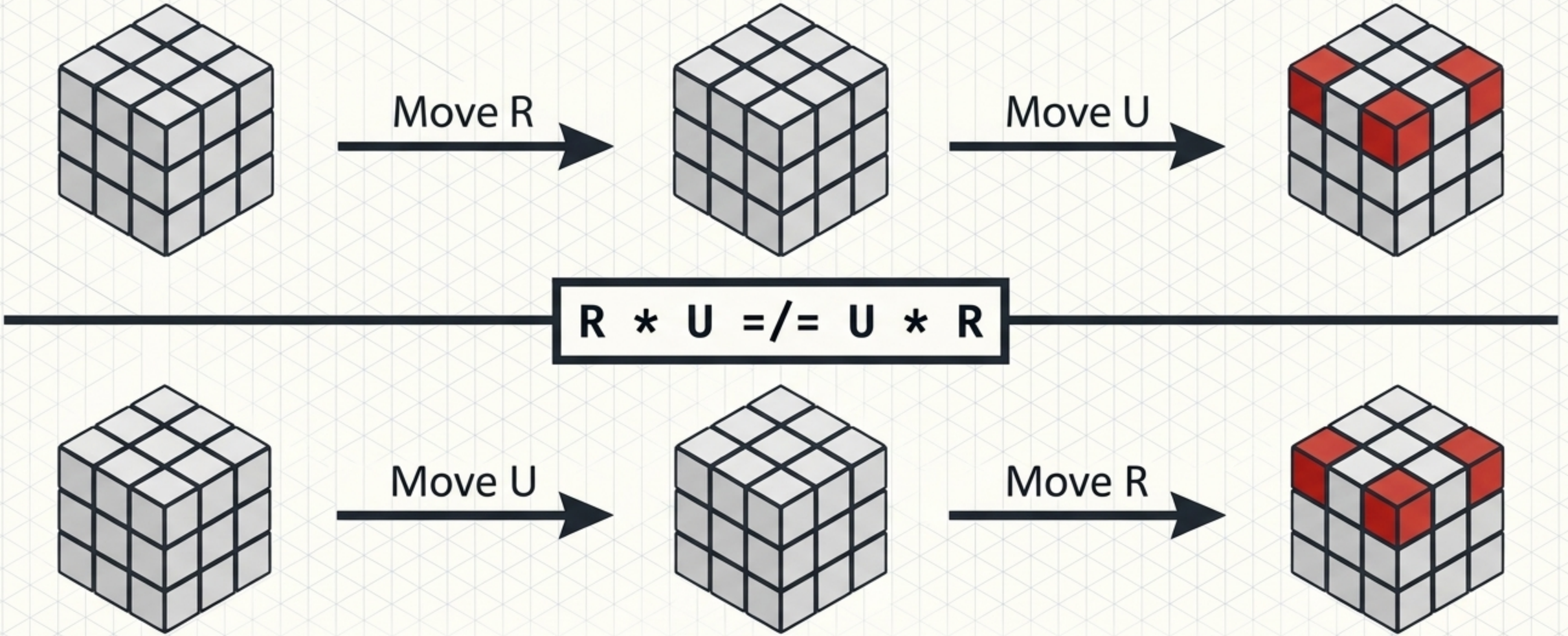


The sequence of length zero. Doing nothing.

Inverses

Every sequence reverses. The inverse of R * U * F is exactly F’ * U’ * R’.

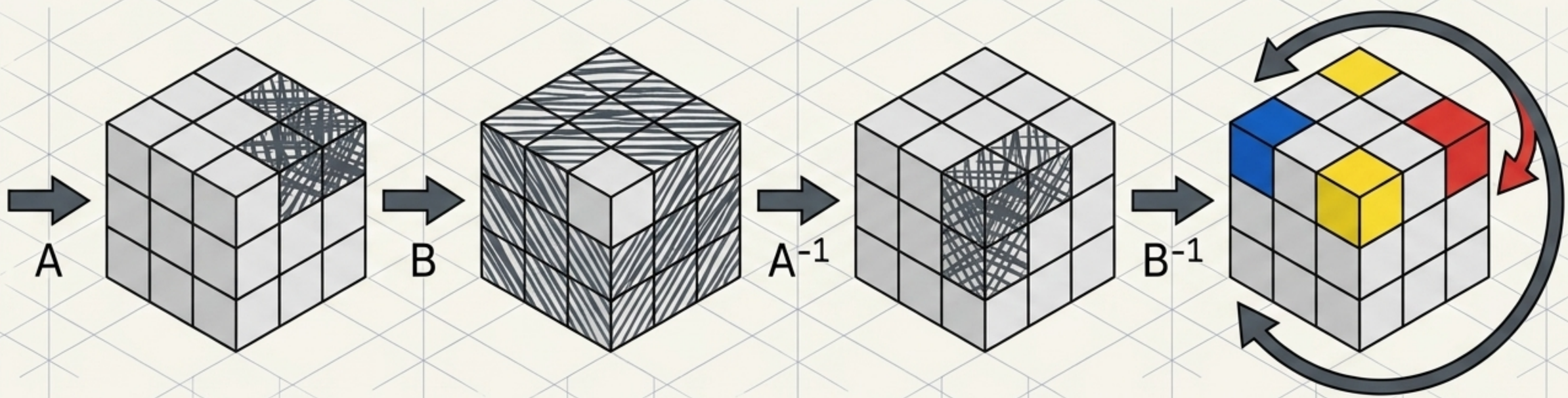
The Non-Abelian Path



Order matters. The Rubik's Cube Group is non-abelian.
Solving one part inevitably disturbs previously solved parts.

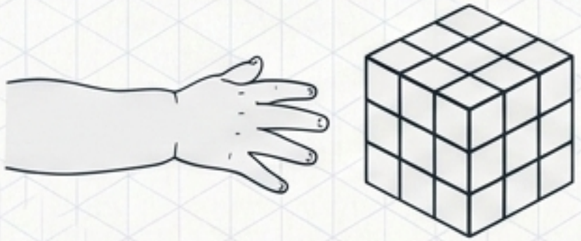
The Commutator Engine

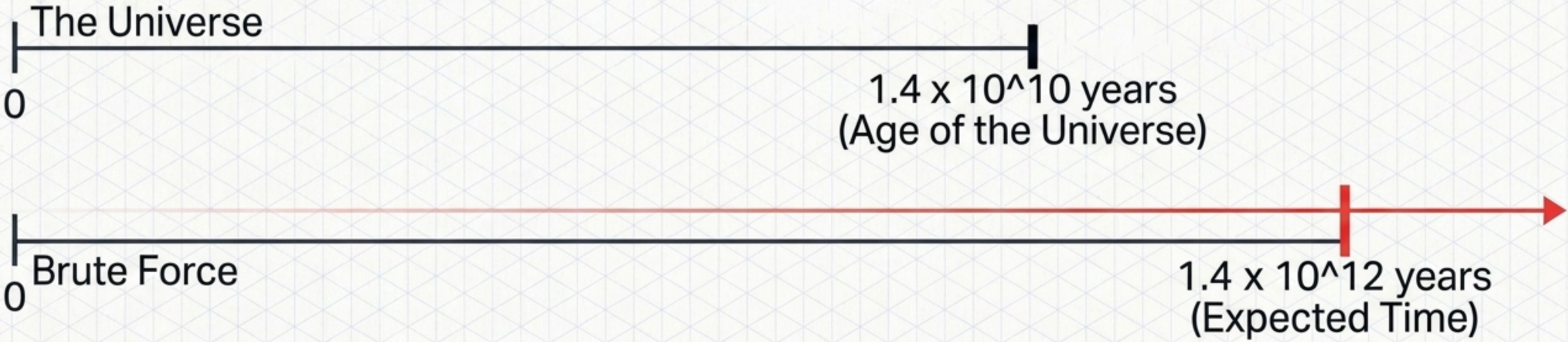
$$[A, B] = A * B * A^{-1} * B^{-1}$$



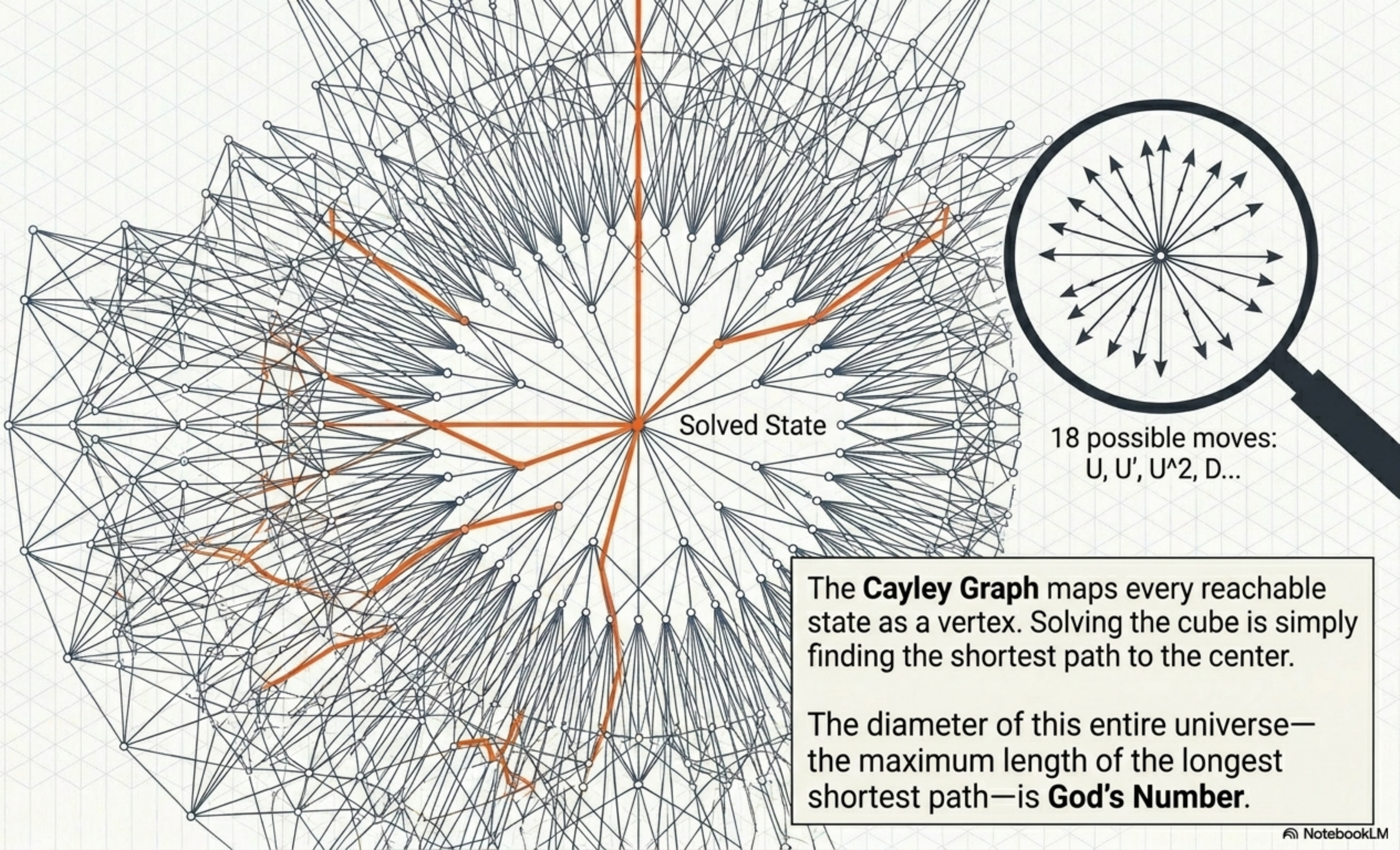
How speedcubers cheat chaos. A commutator measures how far A and B are from commuting. Because most of the permutation algebraically cancels out, it allows us to swap a few targeted pieces while leaving the rest of the puzzle intact.

Can a child raised in isolation solve it by guessing?





A random walk on 4.3 x 10^19 states trying one new state per second takes roughly 100 times the age of the universe. To solve it, you must exploit the group structure.



The **Cayley Graph** maps every reachable state as a vertex. Solving the cube is simply finding the shortest path to the center.

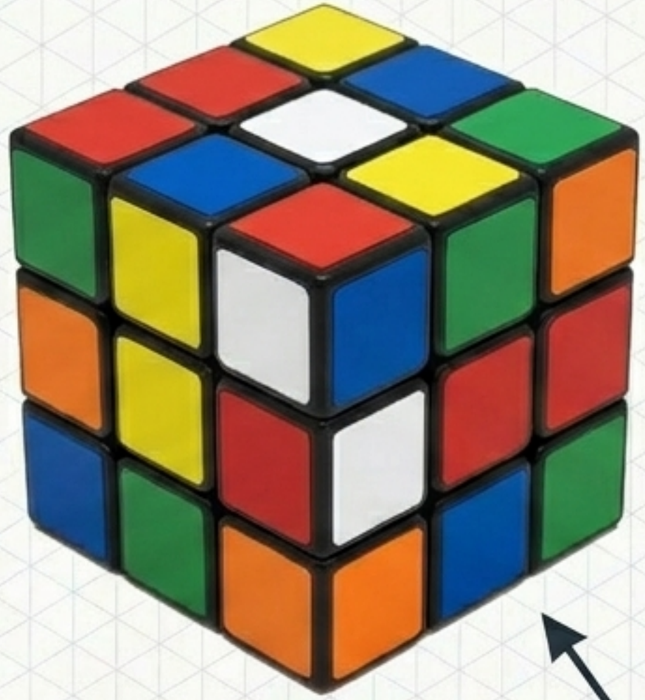
The diameter of this entire universe—the maximum length of the longest shortest path—is **God's Number**.

1981: Lower 18 — Upper 52

1992: Lower 18 — Upper 42

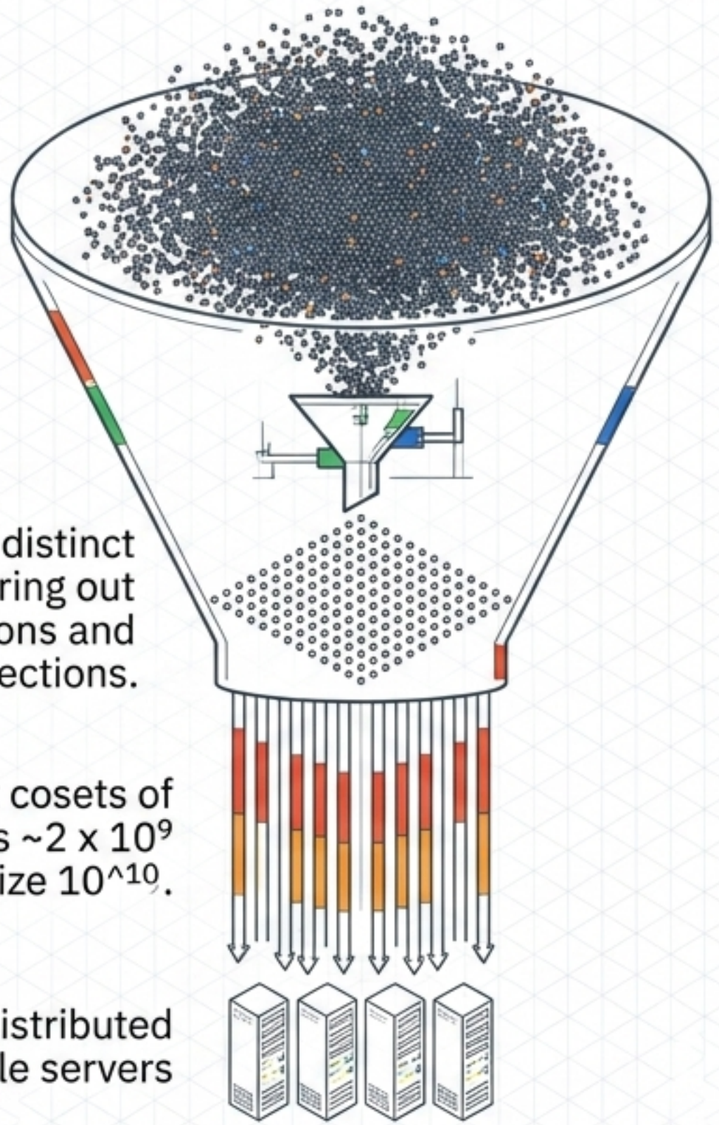
2008: Lower 20 — Upper 26

2010: Lower 20 — Upper 20



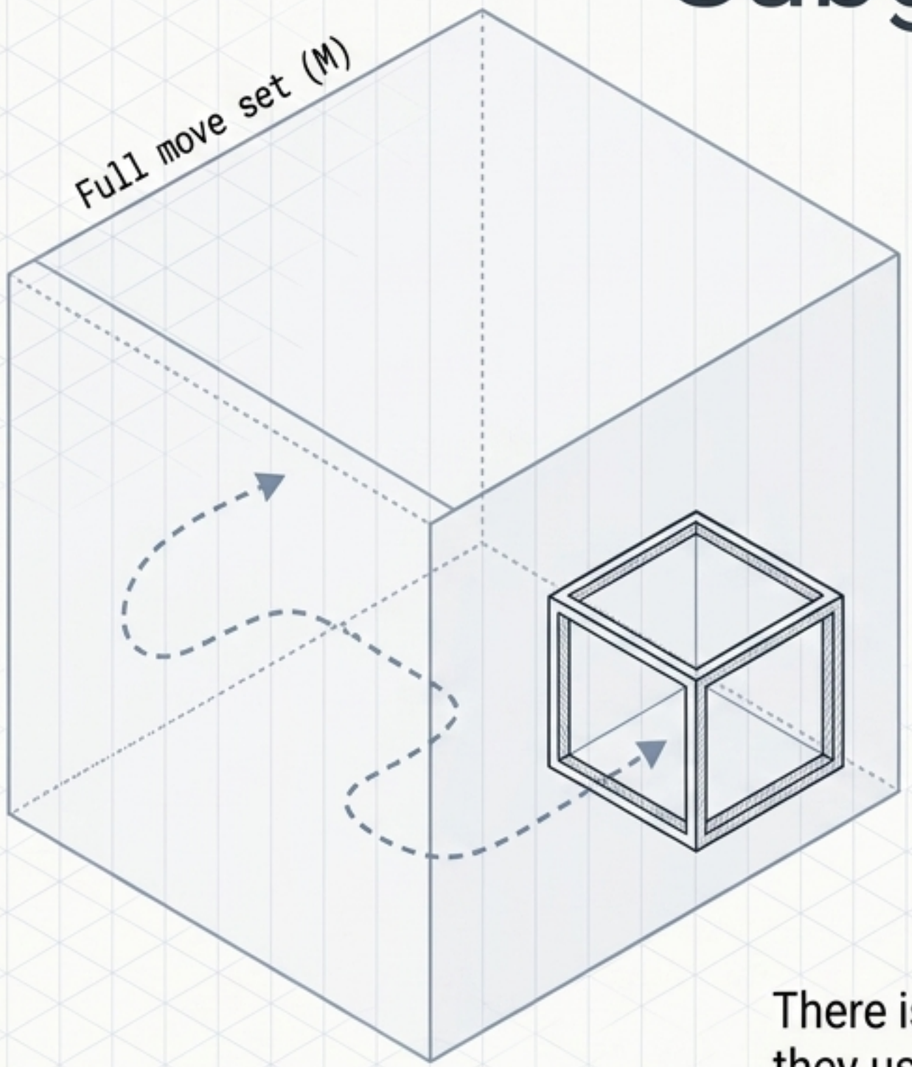
The **Superflip**: A known state requiring exactly 20 moves.

$$[\, G_{\text{God}} = 20 \,]$$

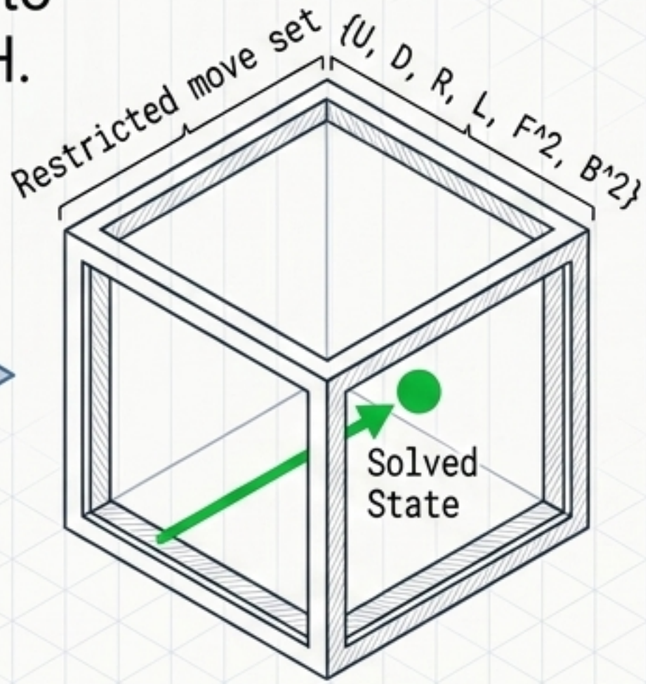


Pure algebra wasn’t enough. Pure computation wasn’t enough.
The proof required combining coset decomposition with distributed servers.

Subgroup Tower



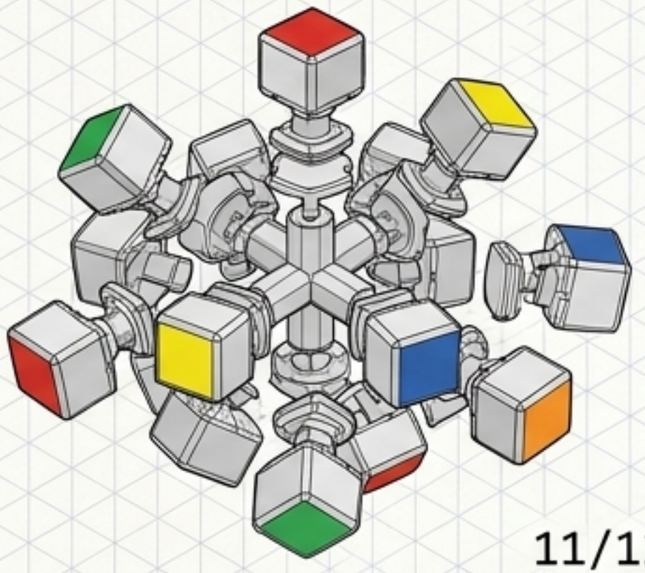
Phase 1:
Navigate into
Subgroup H.

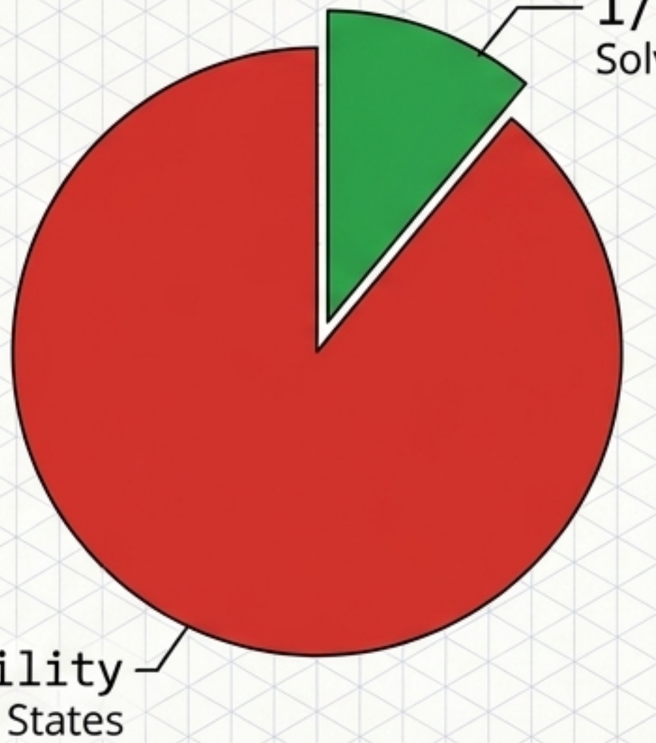


Phase 2:
Navigate to
Solved State.

There is no simple formula. Modern optimal solvers don't use brute force; they use lookup tables to leapfrog through subgroup structures. They solve the coset space, then solve the subgroup. Time to solve: Milliseconds.

Universal Parity





If you disassemble a cube and rebuild it randomly, there is an **11/12 probability** it is physically unsolvable. You cannot swap exactly two corners without swapping two more. Group theory reveals this **parity constraint** before you ever touch the puzzle.

Cryptography

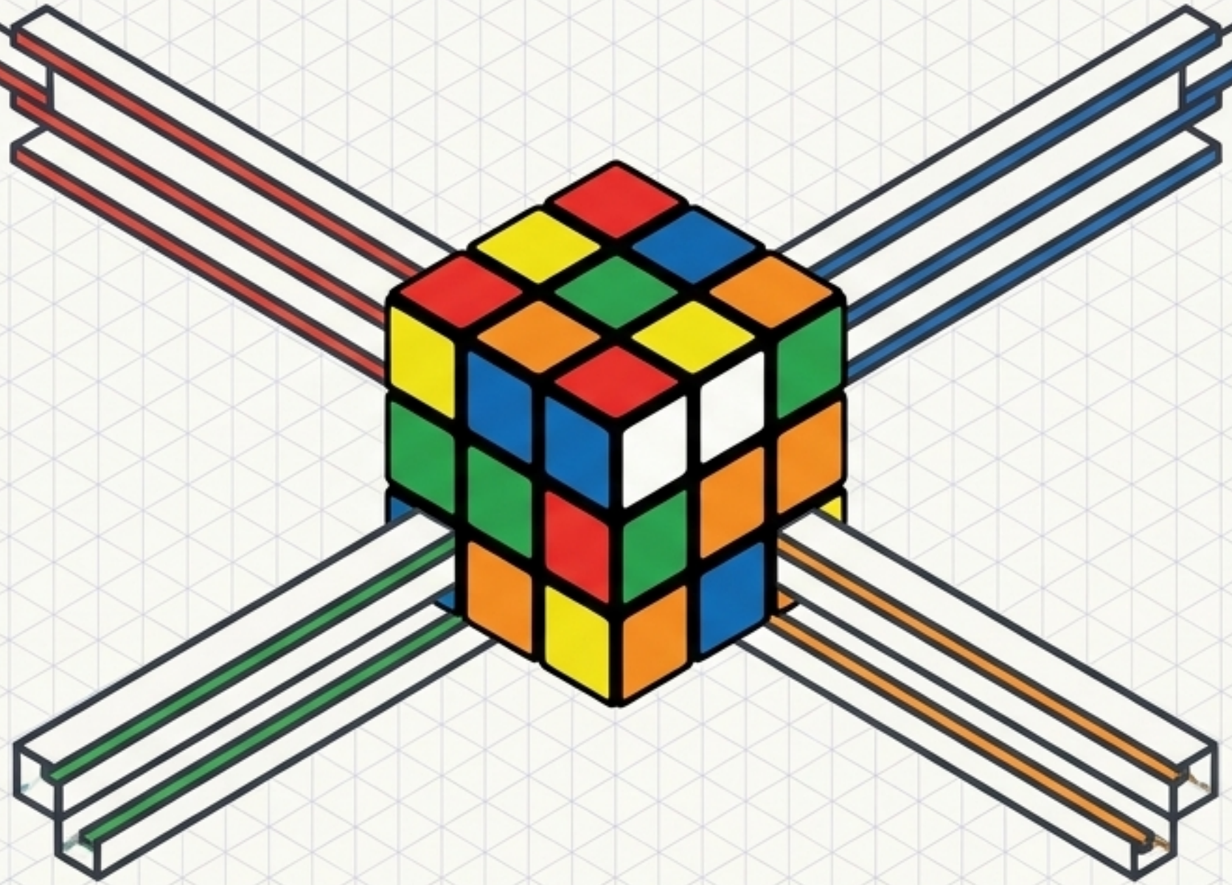
Linked to **Modular Arithmetic**

RSA, Elliptic curves, discrete logarithm hardness.

Particle Physics

Linked to **Subgroups & Representations**

Lie groups U(1), SU(2), SU(3) classifying quarks and leptons.



Error-Correcting Codes

Linked to **Binary Group Parity**

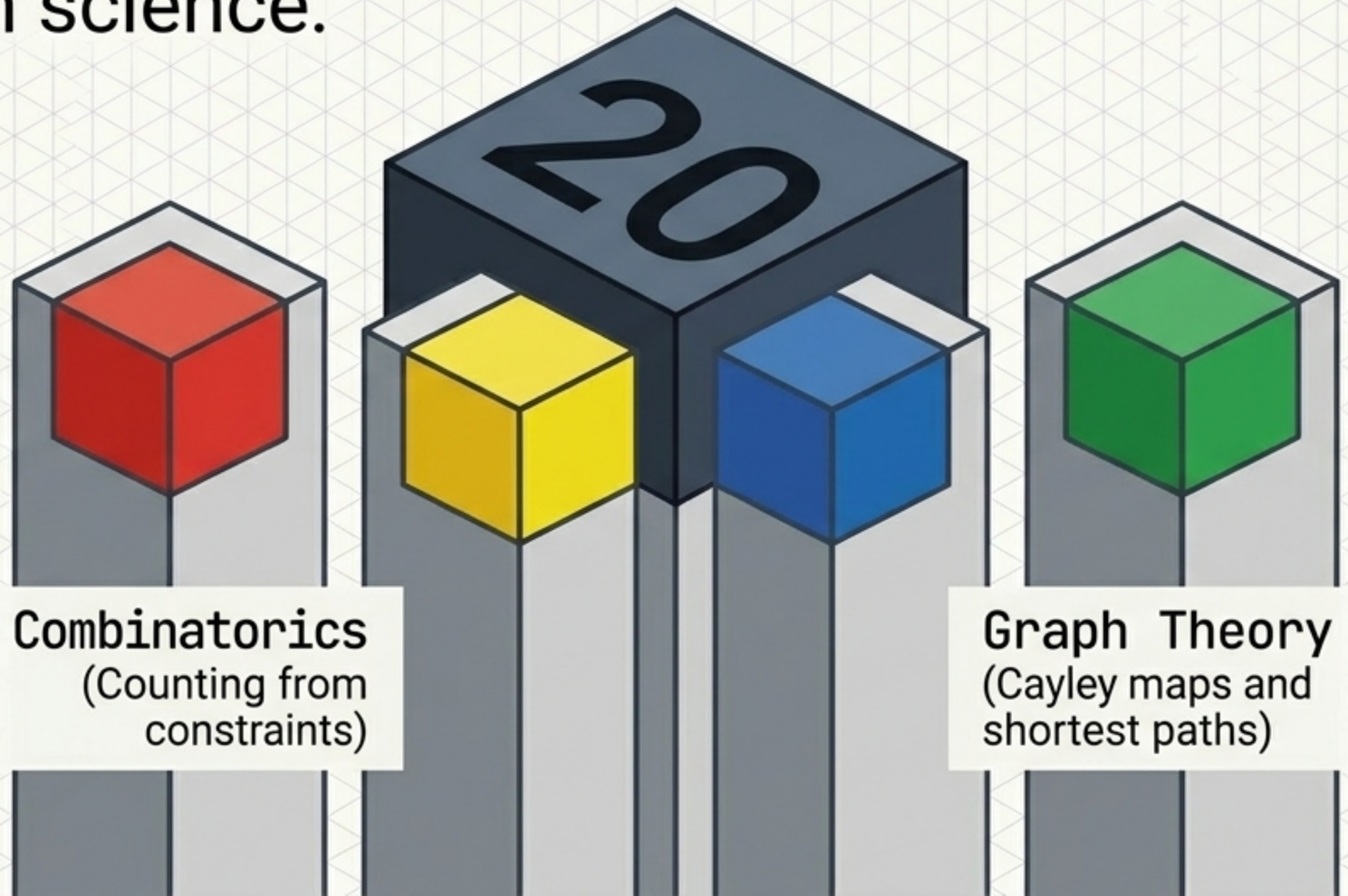
Linear codes as subspaces of F_2^n.

Robotics & 3D Graphics

Linked to **Non-Abelian Rotations**

The SO(3) special orthogonal group governing robot arms.

God's Number is not a curiosity about a toy. It is a **theorem of certainty**. Understanding the **cube** means understanding the **mathematical** architecture of modern science.



Algebraic Structure
(Generators, Subgroups, Cosets)

Combinatorics
(Counting from constraints)

Graph Theory
(Cayley maps and shortest paths)

Computational Complexity
(Distributed solving limits)