Mathematics of the Rubiks' cube

Evgeny Shinder

School of Mathematics and Statistics
University of Sheffield

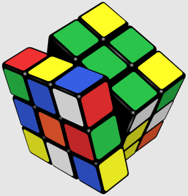
09.02.2016

Plan for today

1. The Rubik's cube
2. Group theory of the cube
3. Complexity of the cube

1. The Rubik's Cube

History of the cube



- Ernő Rubik, hungarian sculptor, inventor and Professor of Architecture created the Cube in 1974
- Since then Rubik's cube is considered as one of the world best-selling toys

Competitions

- First world championship in Budapest, 1982: world record 22 seconds
- Current world record: below 5 seconds
- Blindfolded solving

Structure of the cube

A $3d$ cube has 8 corners, 12 edges, 6 faces (Euler characteristic $= 8 - 12 + 6 = 2$, same as that of a sphere).

Cubies of the Rubik's cube

- 6 center pieces
- 12 edge pieces
- 8 corners

Cube's friends: five platonic solids

Valid and invalid configurations

Valid configurations

A **valid configuration** of the cube is the one that can be obtained by a sequence of face rotations:

$$F, B, R, L, U, D$$

Examples of **invalid** configurations

- Two edge pieces swapped or two corner pieces swapped
- One edge flipped
- One corner twisted

Characterization of valid configurations

Theorem

A configuration is valid if and only if the following three conditions hold:

(1) *Permutations of edge pieces and the permutation of corner pieces have the same parity, i.e. both even or both odd*

(2) *Sum of corner twists is zero in* $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$

(3) *Sum of edge flips in zero is* $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

Remarks on the proof

(1) will see later today, using Group Theory.

(2),(3) done by Rachael Johnson in her MSc project this year, based on existing literature

Example

The **superflip** is a position where all the cubies are in their places, and all the corners are oriented correctly, but all the 8 edges are flipped. According to the Theorem it is a valid configuration. It can be obtained by a sequence of 20 moves: $U\ R2\ F\ B\ R\ B2\ R\ U2\ L\ B2\ R\ U'\ D'\ R2\ F\ R'\ L\ B2\ U2\ F2$.

Number of configurations of the cube

All configurations

- Edges permutations: $12!$
- Edges orientations: 2^{12}
- Corners permutations: $8!$
- Corners orientations: 3^8
- Total: $12! \times 2^{12} \times 8! \times 3^8$

Valid configurations

Edges and corners have same permutation parity, corner twists sum up to zero in $\mathbb{Z}_3$, edge twists sum up to zero in $\mathbb{Z}_2$.

Total number of valid configurations:

$$\frac{12! \times 8! \times 2^{12} \times 3^8}{2 \times 3 \times 2} = 43,252,003,274,489,856,000.$$

2. Group theory of the Rubik's Cube

Two groups associated to the Rubik's cube

The Rubik's group

- Group G consists of all *valid* configurations of the cube, with identity given by solved cube
- Formally: G is generated by words $g_1 \cdots g_n$ with $g_i \in \{F, F', B, B', R, R', L, L', U, U', D, D'\}$, and we set

$$g_1 \cdots g_n = e$$

  if the corresponding sequence of moves does not change the configuration of the cube.

The extended Rubik's group

- Group $\widetilde{G}$ consists of *all* configurations of the cube, including the invalid ones
- We have a subgroup $G = \langle F, B, R, L, U, D \rangle \subset \widetilde{G}$

Both groups G, $\widetilde{G}$ are semi-direct products of certain simpler groups.

Direct applications of group theory

Theorem

- *Every move g of Rubik's cube has finite order: there exists an integer $n > 0$ such that $g^n = e$*
- *There are no moves of prime orders $p \geq 13$.*

Theorem

Flipping just two edges or just two corners is not a valid configuration.

Semi-direct products of groups

Direct (Cartesian) products

- G_1, G_2 groups
- $G_1 \times G_2 = \{(g_1, g_2)\}$
- Pairs are multiplied componentwise:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$$

Semi-direct products

- G_1, G_2 groups
- Given an action of G_2 on G_1: $g_2 \mapsto \phi(g_2) : G_1 \to G_1$
- $G_1 \times G_2 = \{(g_1, g_2)\}$
- Pairs are multiplied using the twist by ϕ:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot \phi_{g_2}(g_1'), g_2 \cdot g_2')$$

- Notation: $G_1 \rtimes G_2$ or $G_1 \rtimes_\phi G_2$

The structure theorems for Rubik's groups

Theorem

The extended Rubik's cube group $\widetilde{G}$ is isomorphic to

$$\big((\mathbb{Z}_2)^{12} \rtimes S_{12}\big) \times \big((\mathbb{Z}_3)^8 \rtimes S_8\big)$$

One can then describe the Rubik's group G as a subgroup inside $\widetilde{G}$. It will consist of quadruples:

$$(x \in \mathbb{Z}_2^{12}, \sigma \in S_{12}, y \in (\mathbb{Z}_3)^8, \tau \in S_8),$$

satisfying:

1. $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau)$
2. $\sum_{i=1}^{12} x_i = 0 \in \mathbb{Z}_3$
3. $\sum_{j=1}^{8} y_j = 0 \in \mathbb{Z}_2$

Using this description one can study group-theoretic properties of the G, $\widetilde{G}$: their centers, subgroups, elements of given order, etc

3. Complexity of the Rubik's Cube

Cayley graph of a group

Let G be a group given with a set of generators $G = \langle t_1, \dots, t_r \rangle$.

Definition

The Cayley graph of G is the graph with:

- Vertices: elements of G
- Edges: we put a directed edge $h \to g$ if $g = t_i h$ for some i

Examples

- Cyclic groups $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_n = \langle \overline{1} \rangle$
- Symmetric group $S_3 = \langle (12), (23) \rangle$
- Rubik's group $G = \langle F, B, R, L, U, D \rangle$, turn metric, or half-turn metric:

$$G = \langle F, F^2, B, B^2, R, R^2, L, L^2, U, U^2, D, D^2 \rangle$$

Diameter of a group

- Diameter of a group G is the diameter of its Cayley graph, i.e. the maximum of the word length required to represent group elements

Diameter of the Rubik's group in half-turn metric

Lower bounds

Lemma

The diameter of the Rubik's group is at least 16, *i.e. some valid configurations require* 16 *face-turn moves to solve.*

Proof.

Proof by contradiction: assume that 15 moves suffices, since the possible number of letters in half-turn metric is 18, the number of words of length 15 is 18^{15}. But we have

$$|G| = 43,252,003,274,489,856,000 > 6,746,640,616,477,458,432 = 18^{15}$$

so we can't possibly exhaust all group elements with words of length 15. □

Theorem

The superflip configuration requires exactly 20 *moves.*

Diameter of the Rubik's group in half-turn metric

Upper bounds

Theorem (M. Davidson, J. Dethridge, H. Kociemba, T. Rokicki, 2010)

The diameter of the Cayley graph of the Rubik's cube with respect to generators

$$F, F^2, B, B^2, R, R^2, L, L^2, U, U^2, D, D^2$$

is equal to 20*. This means that every valid configuration can be solved in at most* 20 *moves, and that some valid configurations require exactly* 20 *moves.*

Remark

In the language of puzzles, the diameter 20 *is referred to as* **God's number***, that is the smallest number needed by God to solve the cube, and the corresponding algorithm is referred to as* **God's algorithm***.*

The proof of the Theorem above relies on efficient and smart computer-based search, taking into account symmetries of the cube...

References

None of what I talked about is my original research. Here are some excellent sources I used for this talk:

1. D. Joyner: *Adventures in Group Theory: Rubiks Cube, Merlins Machine, and Other Mathematical Toys*
2. T. Rokicki: *Twenty-Two Moves Suffice for Rubiks Cube!* http://www.cs.brandeis.edu/~storer/JimPuzzles/RUBIK/Rubik3x3x3/READING/22Moves.pdf

The lower bound on God's number 20 using superflip has been proved by M. Michael in 1995, see http://www.math.rwth-aachen.de/~Martin.Schoenert/Cube-Lovers/michael_reid__superflip_requires_20_face_turns.html.

The upper bound on God's number 20 has been proved by M. Davidson, J. Dethridge, H. Kociemba, T. Rokicki in 2010, see www.cube20.org.

Youtube tutorial I used to learn how to solve the cube: https://www.youtube.com/watch?v=MaltgJGz-dU

Images were taken from the Wikipedia article on Rubik's cube.