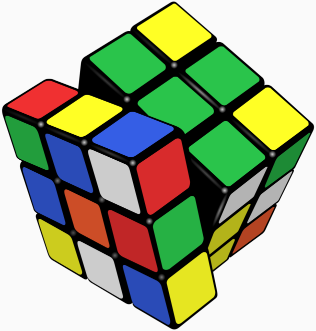
Rubik’s cubes and permutation group theory

Lawrence Chen

October 20, 2022

Honours presentation



Contents

Questions about Rubik's cube

- How can we represent *move sequences* and *states* of a cube?
- How can we tell *how many* states a Rubik's cube can take?
- If we repeat a move, do we eventually *get back to the start*?
- If a Rubik's cube is *restickered*, is it *solvable*?
- How can we use maths to *solve* a Rubik's cube?

One answer: using permutations and *computational group theory*!

(J. A. Paulos, Innumeracy)

> *Ideal Toy Company stated on the package of the original Rubik cube that there were more than three billion possible states the cube could attain. It's analogous to McDonald's proudly announcing that they've sold more than 120 hamburgers.*

Some basic group theory

Permutations

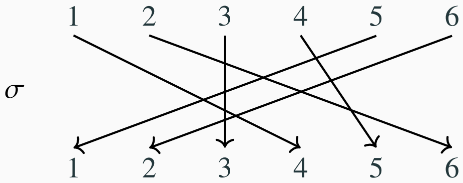
Definition (permutation)

Permutation of $[n] := \{1, \ldots, n\}$ is bijection $\sigma : [n] \to [n]$.

Symmetric group $\mathrm{Sym}(n)$ is set of permutations of $[n]$.

Write $1 = ()$ for identity. Write i^σ not $\sigma(i)$ for *image*.

Cycle notation: $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:

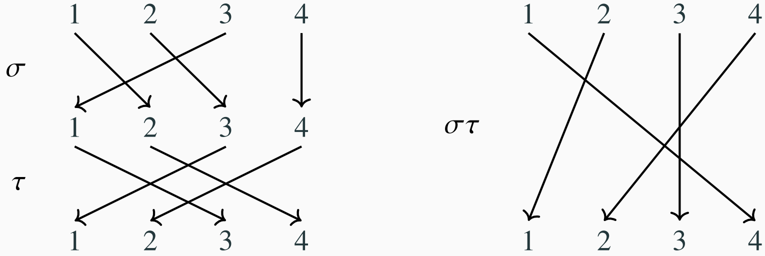


It means

$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,\ 6^\sigma = 2,\ 3^\sigma = 3.$$

Permutations (ii)

Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first σ, then τ”, so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,



$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,2) \in \mathrm{Sym}(4).$$

Note: here, $\sigma\tau \neq \tau\sigma$, since $1^{\sigma\tau} = 4$ but $1^{\tau\sigma} = (1^{\tau})^{\sigma} = 3^{\sigma} = 1$.
Identity $1 = ()$ satisfies $1\sigma = \sigma 1 = \sigma$ for $\sigma \in \mathrm{Sym}(n)$.

Permutation groups

Note: for $\sigma, \tau, \pi \in \mathrm{Sym}(n)$, (i) $\sigma\tau \in \mathrm{Sym}(n)$, (ii) $1 = () \in \mathrm{Sym}(n)$, (iii) $\sigma^{-1} \in \mathrm{Sym}(n)$, (iv) $(\sigma\tau)\pi = \sigma(\tau\pi)$. If true for subset:

Definition (permutation group)

Permutation group of degree n is subset $G \subseteq \mathrm{Sym}(n)$ satisfying:

(i) **(closure)** $\sigma\tau \in G$ for $\sigma, \tau \in G$;

(ii) **(identity)** $1 = () \in G$;

(iii) **(inverses)** $\sigma^{-1} \in G$ for $\sigma \in G$.

Write $G \leq \mathrm{Sym}(n)$.

Example (alternating group)

Alternating group $\mathrm{Alt}(3) = \{(), (1,2,3), (1,3,2)\} \leq \mathrm{Sym}(3)$ is permutation group of degree 3, with $(1,2,3)^{-1} = (1,3,2)$.

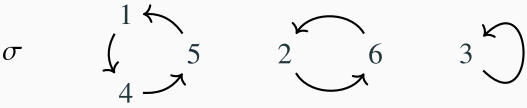
Order of permutations

Definition (order)

Order of $\sigma \in G$ is least $k \in \mathbb{Z}_+$ with $\sigma^k = \sigma \cdots \sigma = 1$.

Example

Consider $\sigma = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$.



Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$, $4^{\sigma^3} = 4$, $5^{\sigma^3} = 5$, $2^{\sigma^2} = 2$, $6^{\sigma^2} = 6$ so $\sigma^6 = () = 1$; order of σ is 6.

Proposition

Order of $\sigma \in \mathrm{Sym}(n)$ *is lcm of cycle lengths.*

Generating a group

Definition (generator)

Set X **generates** G if every $\sigma \in G$ is $\sigma = x_1^{\pm 1} \cdots x_r^{\pm 1}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**; write $G = \langle X \rangle$.

(If $G = \langle X \rangle$ for some $|X|$ with $|X| = 1$, G is **cyclic**.)

Example (cyclic group)

Consider $\mathrm{Alt}(3) = \{(), (1,2,3), (1,3,2)\}$: $(1,2,3)^2 = (1,3,2)$, $(1,2,3)^3 = ()$, so $\mathrm{Alt}(3) = \langle (1,2,3) \rangle$ is cyclic (only for $n = 3$).

Example (symmetric group)

Consider $\mathrm{Sym}(3) = \{(), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. Not cyclic, but $\mathrm{Sym}(3) = \langle (1,2), (2,3) \rangle$ (adjacent swaps). Also, $\mathrm{Sym}(3) = \langle (1,2), (1,2,3) \rangle$, e.g. $(2,3) = (1,2,3)(1,2)$.

Group actions

Definition (group action)

For permutation group G and set $\Omega \neq \emptyset$, G**-action** is map $\Omega \times G \to \Omega$, $(\alpha, \sigma) \mapsto \alpha^\sigma$ s.t. $\alpha^1 = \alpha$ and $\alpha^{\sigma\tau} = (\alpha^\sigma)^\tau$ for $\alpha \in \Omega$ and $\sigma, \tau \in G$.

Idea: $\alpha \in \Omega$ is *state*, apply *move* $\sigma \in G$ to get state $\alpha^\sigma \in \Omega$, in way that respects permutation product.

Example (natural action)

$G \leq \mathrm{Sym}(n)$ acts on $\Omega = [n]$ by $\alpha^\sigma := \alpha^\sigma$ (image) for $\alpha \in [n]$, $\sigma \in G$.

Example (right regular action)

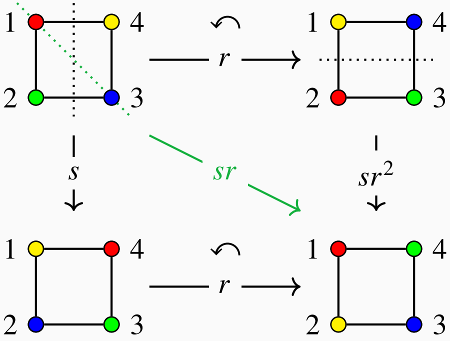
Perm group G acts on $\Omega = G$ (itself) via $\alpha^\sigma := \alpha\sigma$ for $\alpha, \sigma \in G$. (*Check:* $\alpha^1 = \alpha 1 = \alpha$ and $\alpha^{\sigma\tau} = \alpha(\sigma\tau) = (\alpha\sigma)\tau = (\alpha^\sigma)^\tau$.)

Group actions (ii)

Example (dihedral group)

Let $r = (1,2,3,4)$, $s = (1,4)(2,3) \in \mathrm{Sym}(4)$. **Dihedral group** is $D_8 := \langle r, s \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, *"symmetries of square"*.

Note: $sr = (2,4)$, $sr^2 = (1,2)(3,4)$. Action of D_8 on vertices of square (positions labelled by $[4]$): $\sigma \in D_8$ sends vertex at i to i^σ.



Orbits and stabilisers

Definition (orbit)

If G acts on Ω, then **orbit** of $\alpha \in \Omega$ is $\alpha^G := \{\alpha^\sigma : \sigma \in G\}$.

Idea: states $\alpha^\sigma \in \Omega$ reachable from fixed $\alpha \in \Omega$ by moves $\sigma \in G$.

Definition (stabiliser)

If G acts on Ω, then **stabiliser** of $\alpha \in \Omega$ is $G_\alpha := \{\sigma \in G : \alpha^\sigma = \alpha\}$.

Idea: moves $\sigma \in G$ that fix given $\alpha \in \Omega$.

Example (right regular action)

G acts on $\Omega = G$ via $\alpha^\sigma = \alpha\sigma$ for $\alpha, \sigma \in G$. Orbit of $\alpha \in G$ is $\Omega = G$ ($\alpha^{\alpha^{-1}\beta} = \beta \in G$); stabiliser of α is $\{1\} = 1$ ($\alpha\sigma = \alpha \implies \sigma = 1$).

Orbits and stabilisers (ii)

Orbit α^G: states $\alpha^\sigma \in \Omega$ reachable from fixed α by moves $\sigma \in G$.
Stabiliser G_α: moves $\sigma \in G$ that fix given α.

Example (dihedral group)

Recall $G = D_8 = \langle r, s\rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \leq \mathrm{Sym}(4)$ where $r = (1, 2, 3, 4)$, $s = (1, 4)(2, 3)$.

Orbit of 1: $1^1 = 1$, $1^r = 2$, $1^{r^2} = 3$, $1^{r^3} = 4$, so $1^G = [4]$.

Stabiliser of 1: $sr = (2, 4)$, $sr^2 = (1, 2)(3, 4)$, $sr^3 = (1, 3)$, so $G_1 = \{(), (2, 4)\} = \{1, sr\}$.

Note: $|1^G||G_1| = 4 \cdot 2 = 8 = |D_8|$. Coincidence?

Theorem (orbit-stabiliser)

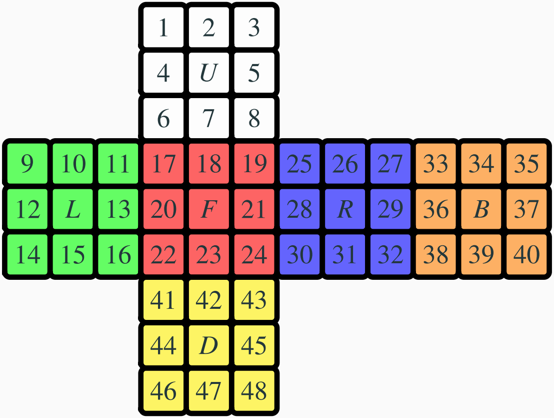
If G acts on Ω, then for $\alpha \in \Omega$, $|\alpha^G||G_\alpha| = |G|$.

The Rubik’s group

Representing the cube and its moves

Rubik's cube has 6 faces, each with 3 × 3 small *facelets*.

In **solved state** 1, label facelets (except each centre) using [48]:

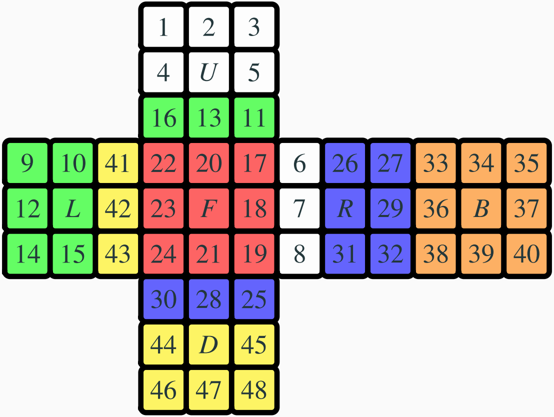


			1	2	3						
			4	*U*	5						
			6	7	8						
9	10	11	17	18	19	25	26	27	33	34	35
12	*L*	13	20	*F*	21	28	*R*	29	36	*B*	37
14	15	16	22	23	24	30	31	32	38	39	40
			41	42	43						
			44	*D*	45						
			46	47	48						

6 **generators** (*moves* in CC): U, L, F, R, B, D (rot. *clockwise*).

Representing the cube and its moves (ii)

From *solved state* 1, consider F which rotates front face clockwise:



			1	2	3						
			4	*U*	5						
			16	13	11						
9	10	41	22	20	17	6	26	27	33	34	35
12	*L*	42	23	*F*	18	7	*R*	29	36	*B*	37
14	15	43	24	21	19	8	31	32	38	39	40
			30	28	25						
			44	*D*	45						
			46	47	48						

Under F: $17 \mapsto 19 \mapsto 24 \mapsto 22 \mapsto 17$, $18 \mapsto 21 \mapsto 23 \mapsto 20 \mapsto 18$, $6 \mapsto 25 \mapsto 43 \mapsto 16 \mapsto 6$, $7 \mapsto 28 \mapsto 42 \mapsto 13 \mapsto 7$, $8 \mapsto 30 \mapsto 41 \mapsto 11 \mapsto 8$, else fixed. So

$$F = (17, 19, 24, 22)(18, 21, 23, 20)(6, 25, 43, 16)(7, 28, 42, 13)(8, 30, 41, 11) \in \mathrm{Sym}(48).$$

Representing the cube and its moves (iii)

Generators as permutations of labels [48]:

- $U = (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19)$
- $L = (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35)$
- $F = (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)$
- $R = (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24)$
- $B = (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27)$
- $D = (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)$

(Valid) move is sequence of generators and inverses. E.g. $RUR^{-1}U^{-1}$, $URU^{-1}L^{-1}UR^{-1}U^{-1}L$, $RUR^{-1}URU^2R^{-1}U^2$.

Empty move is $1 = ()$ (valid: $1 = RR^{-1}$).

Solving is applying valid move to get to solved state 1.

Representing the cube and its moves (iv)

In cubing community: moves called *move sequences*. Inverse generators (also *"moves"* in CC) written U', L', F', R', B', D' (instead of U^{-1} etc.); powers written $U2, R2$ etc. (instead of U^2, R^2).

Recall: $\sigma = \tau$ in $\mathrm{Sym}(n)$ iff $i^\sigma = i^\tau$ for all $i \in [n]$.

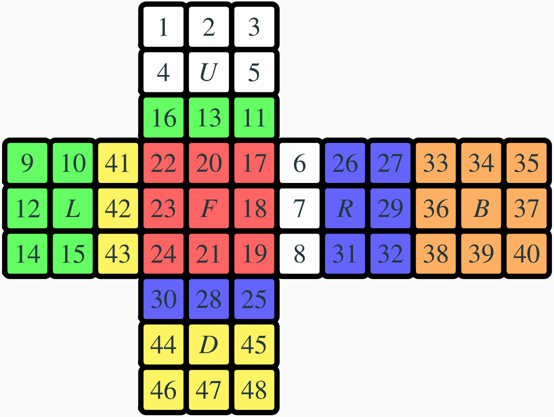
Moves *don't generally commute*: $RU \neq UR$ since

- $R = (25, 27, 32, 30)(26, 29, 31, 28)(3, 38, 43, 19)(5, 36, 45, 21)(8, 33, 48, 24)$
- $U = (1, 3, 8, 6)(2, 5, 7, 4)(9, 33, 25, 17)(10, 34, 26, 18)(11, 35, 27, 19)$

$$19^{RU} = (19^R)^U = 3^U = 8 \quad \text{but} \quad 19^{UR} = (19^U)^R = 11^R = 11.$$

Moves vs states for Rubik's cube

(Valid) state is result of applying *valid move* to *solved state* 1.



			1	2	3						
			4	*U*	5						
			16	13	11						
9	10	41	22	20	17	6	26	27	33	34	35
12	*L*	42	23	*F*	18	7	*R*	29	36	*B*	37
14	15	43	24	21	19	8	31	32	38	39	40
			30	28	25						
			44	*D*	45						
			46	47	48						

This new state is valid, as result of applying *F* to solved state.

Moves vs states for Rubik's cube (ii)

Restickering is valid state iff it can be *solved*. How to check?

Let $\mathcal{S}$ be valid **states**; let state $x \in \mathcal{S}$ be element of $\mathrm{Sym}(48)$ giving permutation of labels to solved state $1 \in \mathcal{S}$.
(I.e. i^x is 1-label of facelet at x-position of facelet i.)

Let $\mathcal{G}$ be valid **moves**; each generator/inverse applied corresponds to turn of that face (determined by centre facelet), holding cube fixed.

- State $x \in \mathcal{S}$ corresponds to move $x \in \mathcal{G}$ required to get solved state 1 into state x.
- Move $\sigma \in \mathcal{G}$ corresponds to state $\sigma \in \mathcal{S}$ reached by applying move σ to solved state 1.

So moves ↔ states; as sets, $\mathcal{S} = \mathcal{G}$. *Solved state* is $1 = () \in \mathrm{Sym}(48)$.

The Rubik's group of permutations

For set of moves $\mathcal{G}$: product of valid moves is valid move; identity $1 = () \in \mathcal{G}$, inverse moves exist (undo generators/inverses).

Definition (Rubik's group)
$\mathcal{G} \leq \mathrm{Sym}(48)$ is permutation group of degree 48, called **Rubik's group**. *Note:* $G = \langle U, L, F, R, B, D \rangle$.

$\mathcal{G}$ acts on non-centre facelets labelled by $[48]$: for $\sigma \in \mathcal{G}$, i^{σ} is 1-label on facelet that σ sends facelet i to, from solved state 1. (This corresponds to *natural action* as perm group; c.f. D_8-action earlier.)

For *move* $\sigma \in \mathcal{G}$ and *state* $x \in \mathcal{S}$, applying σ to x gives *state* $x^{\sigma} = x\sigma \in \mathcal{S}$. This is *regular action* of $\mathcal{G}$. (Consider states $x \in \mathcal{G}$.)

Clearly $\mathcal{G}$ finite (states ↔ moves; also $|\mathcal{G}| \leq 48!$). But what is $|\mathcal{G}|$?

The Rubik’s group of permutations (ii)

`GAP` code to define generators and $\mathcal{G} = \langle U, L, F, R, B, D \rangle$ (as `G`):

```
U := ( 1, 3, 8, 6)( 2, 5, 7, 4)( 9,33,25,17)(10,34,26,18)
     (11,35,27,19);;
L := ( 9,11,16,14)(10,13,15,12)( 1,17,41,40)( 4,20,44,37)(
     6,22,46,35);;
F := (17,19,24,22)(18,21,23,20)( 6,25,43,16)( 7,28,42,13)(
     8,30,41,11);;
R := (25,27,32,30)(26,29,31,28)( 3,38,43,19)( 5,36,45,21)(
     8,33,48,24);;
B := (33,35,40,38)(34,37,39,36)( 3, 9,46,32)( 2,12,47,29)(
     1,14,48,27);;
D := (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)
     (16,24,32,40);;
G := Group( U, L, F, R, B, D );
```

`Order` cmd: $|\mathcal{G}| = 43\,252\,003\,274\,489\,856\,000 \approx 4.3 \cdot 10^{19}$. *How?*

Analysing the Rubik’s group

Concluding remarks

References and resources

- Analyzing Rubik's cube with GAP: `https://www.gap-system.org/Doc/Examples/rubik.html`
- J.A. Paulos — *Innumeracy* (book)
- Holt — *Handbook of Computational Group Theory* (textbook)
- Dixon and Mortimer — *Permutation Groups* (textbook)
- Orders of elements in Rubik's group (1260 largest, 13 smallest without, 11 rarest, 60 most common, median 67.3, 73 options): `https://www.jaapsch.net/puzzles/cubic3.htm#p34`
- Thistlethwaite's 52 move algorithm (using group theory): `https://www.jaapsch.net/puzzles/thistle.htm`