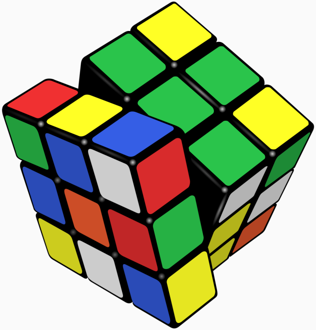
Rubik's cubes and permutation group theory

Lawrence Chen

October 9, 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

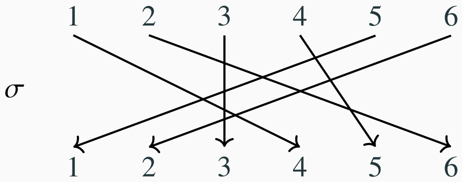
Definition (permutation)

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:

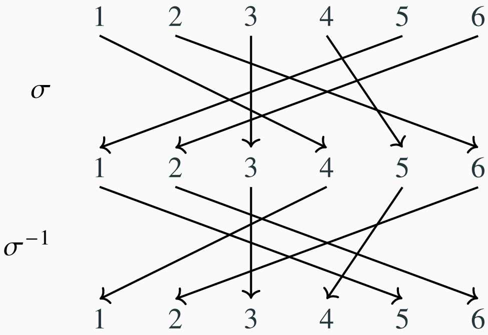


It means

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

Permutations (ii)

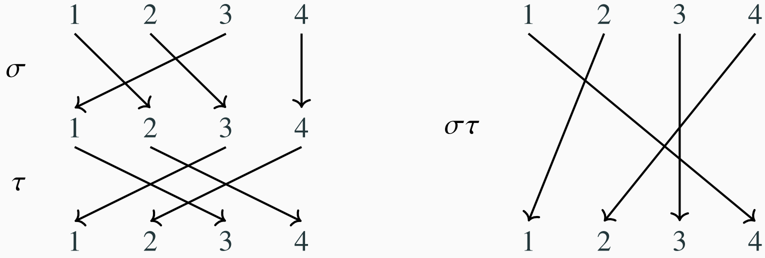
Inverses: For $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$:



Inverse is $\sigma^{-1} = (1,5,4)(2,6) \in \mathrm{Sym}(6)$.

Permutations (iii)

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

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.

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 $\alpha \in [n]$, $\sigma \in G$.

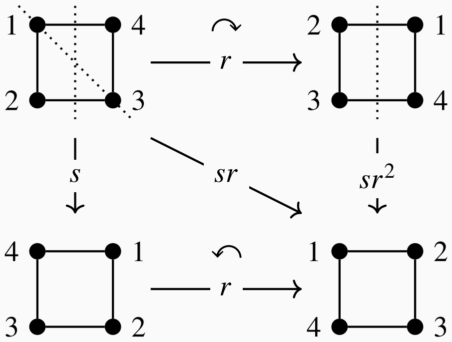
Example (right regular action)

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 $\alpha^{\sigma\tau} = \alpha(\sigma\tau) = (\alpha\sigma)\tau = (\alpha^\sigma)^\tau$.)

Example (dihedral group)

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

Note: $sr = (2, 4)$, $sr^2 = (1, 2)(3, 4)$. Natural action of D_8 on $[4]$:



Group actions (iii)

Definition (orbit)

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

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

Definition (stabiliser)

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

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

Example (right regular action)

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

Definition (orbit, stabiliser (again))

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

Note: stabiliser G_α is subgroup of G. (So G_α acts on Ω.)

Example (Natural action)

$G = \{(), (1,2,4), (1,4,2)\} \leq \mathrm{Sym}(4)$ acts on $\Omega = [4]$ naturally.
Orbit of 1 is $1^G = \{1,2,4\}$, stabiliser of 1 is $G_1 = \{()\} = 1$. Orbit of 3 is $3^G = \{3\}$, stabiliser of 3 is $G_3 = G$.

Note: $|1^G||G_1| = 3 \cdot 1 = 3 = |G|$, $|3^G||G_3| = 1 \cdot 3 = 3 = |G|$.

Theorem (orbit-stabiliser)

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

The Rubik’s group

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`