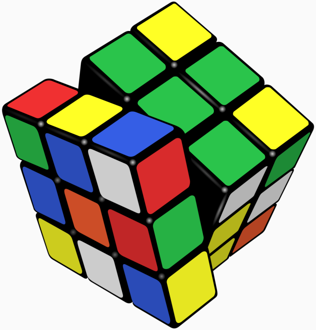
Minimum bases in permutation groups

Lawrence Chen

October 20, 2022

Honours presentation



Contents

Motivation: understanding the Rubik's cube

- How can we represent *operations* of a cube?
- How can we tell *how many* states a Rubik's cube can take?
- How can we better *understand* operations of a 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

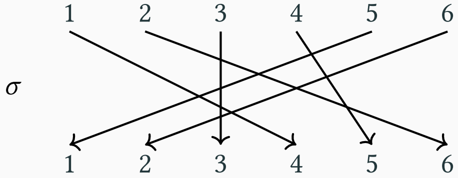
Definition (permutation)

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:

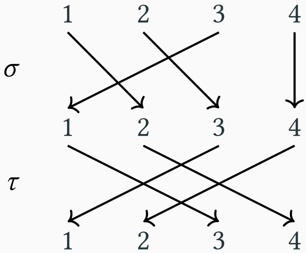


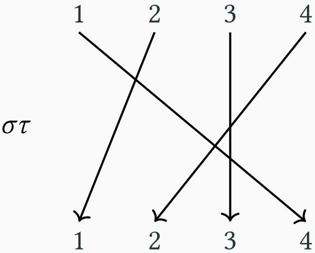
It means

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

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 $G \leq \mathrm{Sym}(n)$ satisfying:

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

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

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

Example (alternating group)

Alternating group $\mathrm{Alt}(3) = \{(), (1,2,3), (1,3,2)\} < \mathrm{Sym}(3)$.

In general, $\mathrm{Alt}(n)$ is all *even* permutations of $[n]$ (product of even # of *transpositions* (i, j), e.g. $(1,2,3) = (1,2)(1,3)$).

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 $\Omega \neq \emptyset$, a 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 $\alpha \in [n]$, $\sigma \in G$.

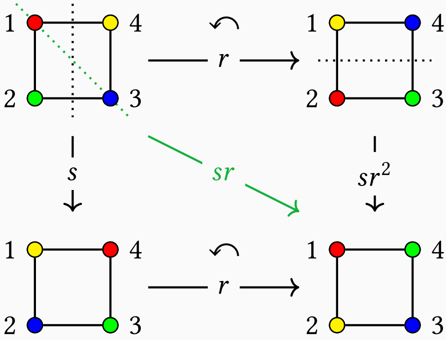
Example (right regular action)

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 $D_8 := \langle r, s\rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, *"symmetries of square"*.

Note: $sr = (2,4)$, $sr^2 = (1,2)(3,4)$. Action of D_8 on vertices of square (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 (natural action)

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

One orbit only: **transitive** action.

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 $1^G = [4]$ (transitive).

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

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

Theorem (orbit-stabiliser)

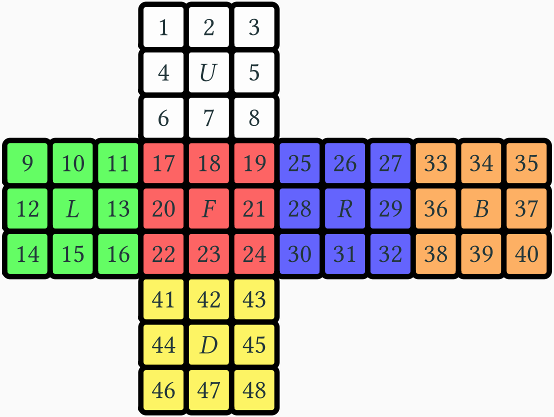
If G acts on Ω, then for $\alpha \in \Omega$, $|\alpha^G||G_\alpha| = |G|$.

The Rubik's group

Representing the cube and its operations

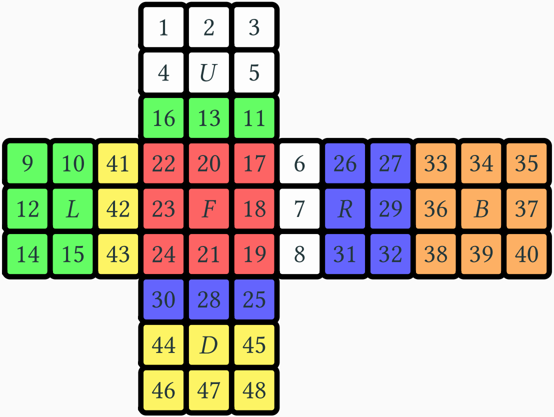
Rubik's cube has 6 faces, each with 3×3 small *stickers*.

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



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

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



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

Representing the cube and its operations (iii)

Generators as permutations of labels [48]:

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

Operation 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 operation is $1 = ()$.

The Rubik's group of permutations

For set of operations $\mathcal{G}$: product of operations is operations; identity $1 = () \in \mathcal{G}$, inverse operations 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:* $\mathcal{G} = \langle U, L, F, R, B, D \rangle$.

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

Clearly $\mathcal{G}$ finite, 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?*

Transitivity and primitivity

Transitive

Transitivity and primitivity (ii)

Blocks, primitive

Transitivity and primitivity (iii)

Example for Rubik's group

Bases and stabiliser chains

Primitive subgroups of affine groups

Affine groups

Definition

Definition

Large base permutation groups (ii)

Liebeck

Moscatiello, Roney-Dougal

Main result

Statement

Main result (ii)

Approach (dot points/observations)

Main result (iii)

Conjecture

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`