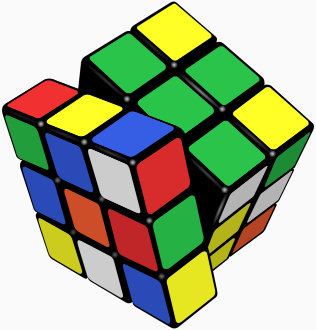
Minimum bases in permutation groups

Lawrence Chen

October 22, 2022

Honours presentation



Contents

Motivation: understanding the Rubik's cube

- How can we represent *operations* of a cube?

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?

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?

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*!

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

Definition (permutation)

Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \dots, n\}$, write $\mathrm{Sym}(n)$.)

Definition (permutation)

Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \ldots, n\}$, write $\mathrm{Sym}(n)$.)

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

Definition (permutation)

Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \ldots, n\}$, write $\mathrm{Sym}(n)$.)

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:

$$\begin{array}{ccccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \sigma & & & & & & \\ & 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

It means

Permutations

Definition (permutation)

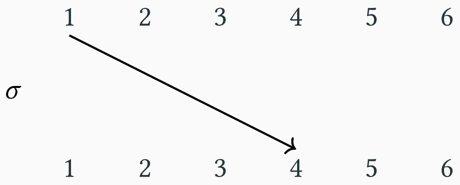
Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \ldots, n\}$, write $\mathrm{Sym}(n)$.)

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 $1^\sigma = 4$,

Permutations

Definition (permutation)

Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \ldots, n\}$, write $\mathrm{Sym}(n)$.)

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:

$$\begin{tikzcd}
{} \arrow[d, phantom, "\sigma"] & 1 \arrow[drrr] & 2 & 3 & 4 \arrow[dr] & 5 & 6 \\
{} & 1 & 2 & 3 & 4 & 5 & 6
\end{tikzcd}$$

It means $1^\sigma = 4,\ 4^\sigma = 5,$

Permutations

Definition (permutation)

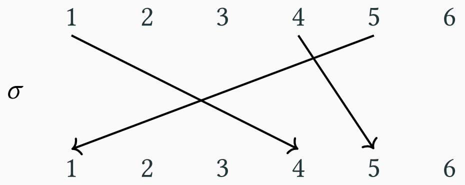
Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \ldots, n\}$, write $\mathrm{Sym}(n)$.)

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 $1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,$

Permutations

Definition (permutation)

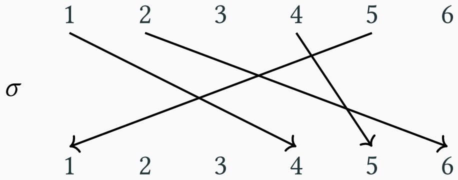
Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \ldots, n\}$, write $\mathrm{Sym}(n)$.)

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

Permutations

Definition (permutation)

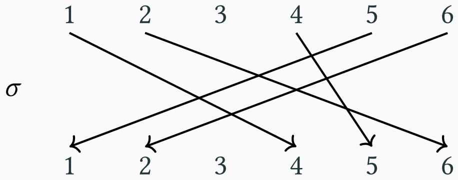
Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \dots, n\}$, write $\mathrm{Sym}(n)$.)

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

Permutations

Definition (permutation)

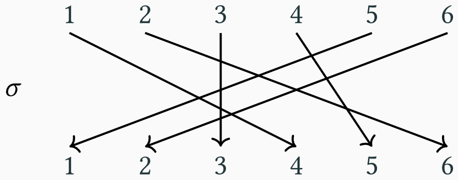
Permutation of Ω is bijection $\sigma : \Omega \to \Omega$.

Symmetric group $\mathrm{Sym}(\Omega)$ is set of permutations of Ω.

(For $\Omega = [n] := \{1, \ldots, n\}$, write $\mathrm{Sym}(n)$.)

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:



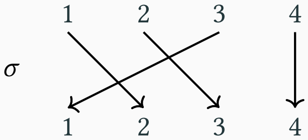
It means $1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,\ 6^\sigma = 2,\ 3^\sigma = 3.$

Permutations (ii)

Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$.

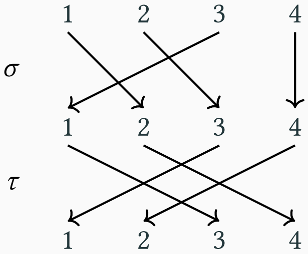
Permutations (ii)

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. $\sigma = (1, 2, 3)$,

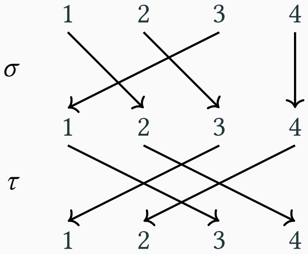


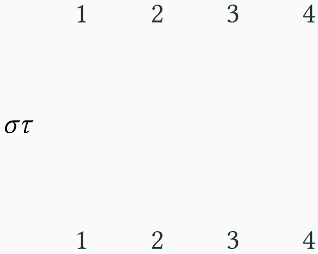
Permutations (ii)

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



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

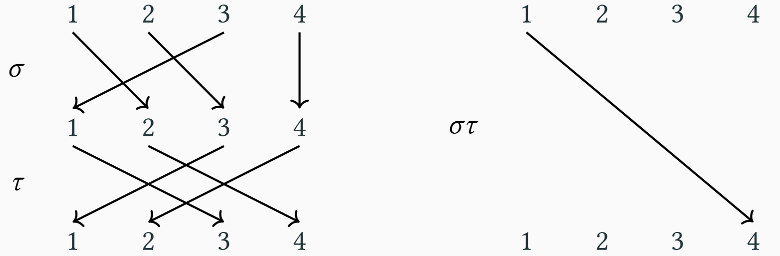




$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,$$

Permutations (ii)

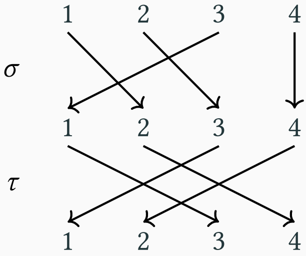
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3)$, $\tau = (1, 3)(2, 4) \in \mathrm{Sym}(4)$,

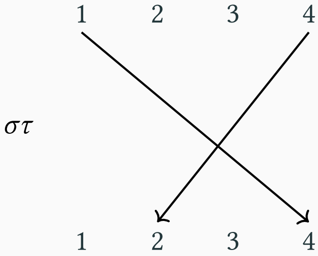


$$\sigma\tau = (1, 2, 3)(1, 3)(2, 4) = (1, 4,$$

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

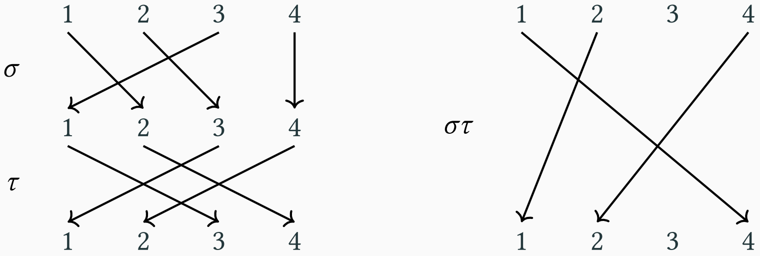




$$\sigma\tau = (1, 2, 3)(1, 3)(2, 4) = (1, 4, 2$$

Permutations (ii)

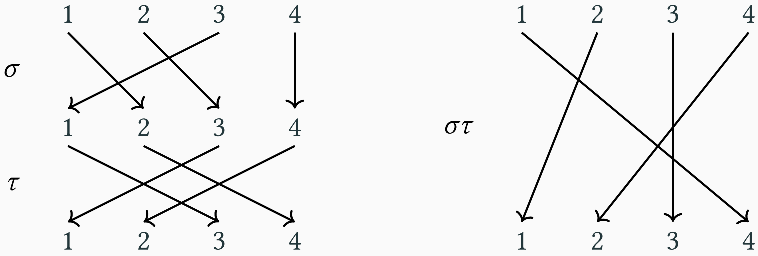
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3)$, $\tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,



$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,2)$$

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 $g, h, k \in \mathrm{Sym}(\Omega)$, (i) $gh \in \mathrm{Sym}(\Omega)$, (ii) $1 = () \in \mathrm{Sym}(\Omega)$, (iii) $g^{-1} \in \mathrm{Sym}(\Omega)$, (iv) $(gh)k = g(hk)$. If true for subset:

Note: for $g, h, k \in \mathrm{Sym}(\Omega)$, (i) $gh \in \mathrm{Sym}(\Omega)$, (ii) $1 = () \in \mathrm{Sym}(\Omega)$, (iii) $g^{-1} \in \mathrm{Sym}(\Omega)$, (iv) $(gh)k = g(hk)$. If true for subset:

Definition (permutation group)

Perm group on Ω (of deg n) is subset $G \leq \mathrm{Sym}(\Omega)$ ($|\Omega| = n$) s.t.

(i) **(closure)** $gh \in G$ for $g, h \in G$;

Permutation groups

Note: for $g, h, k \in \mathrm{Sym}(\Omega)$, (i) $gh \in \mathrm{Sym}(\Omega)$, (ii) $1 = () \in \mathrm{Sym}(\Omega)$, (iii) $g^{-1} \in \mathrm{Sym}(\Omega)$, (iv) $(gh)k = g(hk)$. If true for subset:

Definition (permutation group)

Perm group on Ω (of deg n) is subset $G \leq \mathrm{Sym}(\Omega)$ ($|\Omega| = n$) s.t.

(i) **(closure)** $gh \in G$ for $g, h \in G$;

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

Permutation groups

Note: for $g, h, k \in \mathrm{Sym}(\Omega)$, (i) $gh \in \mathrm{Sym}(\Omega)$, (ii) $1 = () \in \mathrm{Sym}(\Omega)$, (iii) $g^{-1} \in \mathrm{Sym}(\Omega)$, (iv) $(gh)k = g(hk)$. If true for subset:

Definition (permutation group)

Perm group on Ω (of deg n) is subset $G \leq \mathrm{Sym}(\Omega)$ ($|\Omega| = n$) s.t.

(i) **(closure)** $gh \in G$ for $g, h \in G$;

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

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

Permutation groups

Note: for $g, h, k \in \mathrm{Sym}(\Omega)$, (i) $gh \in \mathrm{Sym}(\Omega)$, (ii) $1 = () \in \mathrm{Sym}(\Omega)$, (iii) $g^{-1} \in \mathrm{Sym}(\Omega)$, (iv) $(gh)k = g(hk)$. If true for subset:

Definition (permutation group)

Perm group on Ω (of deg n) is subset $G \leq \mathrm{Sym}(\Omega)$ ($|\Omega| = n$) s.t.

(i) **(closure)** $gh \in G$ for $g, h \in G$;

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

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

Example (alternating group)

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

Permutation groups

Note: for $g, h, k \in \mathrm{Sym}(\Omega)$, (i) $gh \in \mathrm{Sym}(\Omega)$, (ii) $1 = () \in \mathrm{Sym}(\Omega)$, (iii) $g^{-1} \in \mathrm{Sym}(\Omega)$, (iv) $(gh)k = g(hk)$. If true for subset:

Definition (permutation group)

Perm group on Ω (of deg n) is subset $G \leq \mathrm{Sym}(\Omega)$ ($|\Omega| = n$) s.t.

(i) **(closure)** $gh \in G$ for $g, h \in G$;

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

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

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. $(1,2,3) = (1,2)(1,3) \in \mathrm{Sym}(n)$).

Definition (generator)

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

Generating a group

Definition (generator)

Set X **generates** G if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ 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**.)

Generating a group

Definition (generator)

Set X **generates** G if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ 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 $n = 3$).

Generating a group

Definition (generator)

Set X **generates** G if every $g \in G$ is $g = x_1^{\pm 1} \cdots x_r^{\pm 1}$ 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 (perm) group G and set $\Omega \neq \emptyset$, a G-**action** is map $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$. **Degree** of action is $|\Omega|$.

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

Group actions

Definition (group action)

For (perm) group G and set $\Omega \neq \emptyset$, a G-**action** is map $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$. **Degree** of action is $|\Omega|$.

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

Example (natural action)

$G \leq \mathrm{Sym}(\Omega)$ acts on Ω by $\alpha^g := \alpha^g$ (image) for $\alpha \in \Omega$, $g \in G$.

Group actions

Definition (group action)

For (perm) group G and set $\Omega \neq \emptyset$, a G-**action** is map $\Omega \times G \to \Omega$, $(\alpha, g) \mapsto \alpha^g$ s.t. $\alpha^1 = \alpha$ and $\alpha^{gh} = (\alpha^g)^h$ for $\alpha \in \Omega$ and $g, h \in G$. **Degree** of action is $|\Omega|$.

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

Example (natural action)

$G \leq \mathrm{Sym}(\Omega)$ acts on Ω by $\alpha^g := \alpha^g$ (image) for $\alpha \in \Omega$, $g \in G$.

Example (right regular action)

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

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"*.

Example (dihedral group)

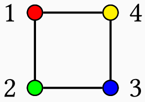
Let $r = (1, 2, 3, 4)$, $s = (1, 4)(2, 3) \in \mathrm{Sym}(4)$. **Dihedral group** is $D_8 := \langle r, s \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, *"symmetries of square"*.

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

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]): $g \in D_8$ sends vertex at i to i^g.

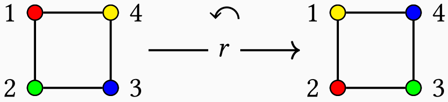


Group actions (ii)

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"*.

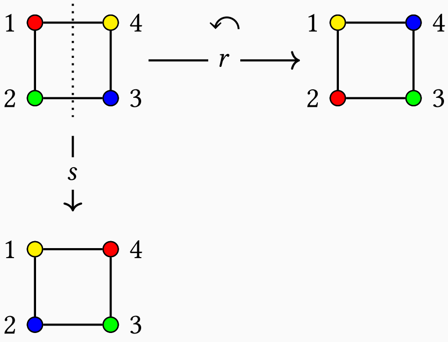
Note: $sr = (2,4)$, $sr^2 = (1,2)(3,4)$. Action of D_8 on vertices of square (labelled by $[4]$): $g \in D_8$ sends vertex at i to i^g.



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"*.

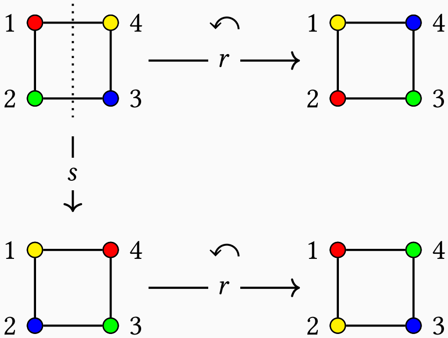
Note: $sr = (2, 4)$, $sr^2 = (1, 2)(3, 4)$. Action of D_8 on vertices of square (labelled by [4]): $g \in D_8$ sends vertex at i to i^g.



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"*.

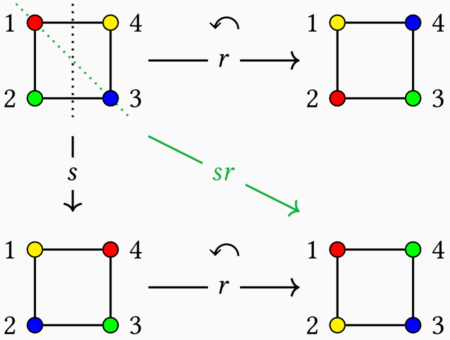
Note: $sr = (2, 4)$, $sr^2 = (1, 2)(3, 4)$. Action of D_8 on vertices of square (labelled by $[4]$): $g \in D_8$ sends vertex at i to i^g.



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"*.

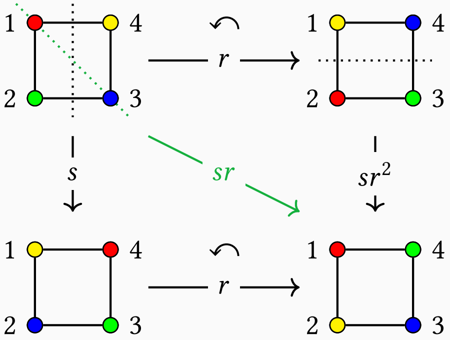
Note: $sr = (2,4)$, $sr^2 = (1,2)(3,4)$. Action of D_8 on vertices of square (labelled by $[4]$): $g \in D_8$ sends vertex at i to i^g.



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 $[4]$): $g \in D_8$ sends vertex at i to i^g.



Orbits and stabilisers

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 $g \in G$.

Orbits and stabilisers

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 $\alpha \in \Omega$.

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 (natural action)

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

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 (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

Orbits and stabilisers

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 (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 $\alpha^g \in \Omega$ reachable from fixed α by moves $g \in G$.

Stabiliser G_α: moves $g \in G$ 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).

Orbits and stabilisers (ii)

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

Stabiliser G_α: moves $g \in G$ 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 $G_1 = \{(), (2, 4)\} = \{1, sr\}$.

Orbits and stabilisers (ii)

Orbit α^G: states $\alpha^g \in \Omega$ reachable from fixed α by moves $g \in G$.
Stabiliser G_α: moves $g \in G$ 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?

Orbits and stabilisers (ii)

Orbit α^G: states $\alpha^g \in \Omega$ reachable from fixed α by moves $g \in G$.
Stabiliser G_α: moves $g \in G$ 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 $\alpha \in \Omega$, $|\alpha^G||G_\alpha| = |G|$.

Blocks and primitivity

Definition (block)

If G acts transitively on Ω and $\Delta \subseteq \Omega$, let $\Delta^g := \{\alpha^g : \alpha \in \Delta\}$.

A **block** is $\Delta \subseteq \Omega$ with $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

Blocks and primitivity

Definition (block)

If G acts transitively on Ω and $\Delta \subseteq \Omega$, let $\Delta^g := \{\alpha^g : \alpha \in \Delta\}$.
A **block** is $\Delta \subseteq \Omega$ with $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

Block is **nontrivial** if $|\Delta| > 1$ and $\Delta \neq \Omega$.

Examples of blocks: singletons, Ω, orbits.

Blocks and primitivity

Definition (block)

If G acts transitively on Ω and $\Delta \subseteq \Omega$, let $\Delta^g := \{\alpha^g : \alpha \in \Delta\}$.
A **block** is $\Delta \subseteq \Omega$ with $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

Block is **nontrivial** if $|\Delta| > 1$ and $\Delta \neq \Omega$.

Examples of blocks: singletons, Ω, orbits.

Definition (primitivity)

A *transitive* G-action is **primitive** if there are no nontrivial blocks; otherwise it is **imprimitive**.

If G is perm group with primitive natural action, G is **primitive**.

Definition (block)

If G acts transitively on Ω and $\Delta \subseteq \Omega$, let $\Delta^g := \{\alpha^g : \alpha \in \Delta\}$.
A **block** is $\Delta \subseteq \Omega$ with $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

Block is **nontrivial** if $|\Delta| > 1$ and $\Delta \neq \Omega$.

Examples of blocks: singletons, Ω, orbits.

Definition (primitivity)

A *transitive* G-action is **primitive** if there are no nontrivial blocks; otherwise it is **imprimitive**.

If G is perm group with primitive natural action, G is **primitive**.

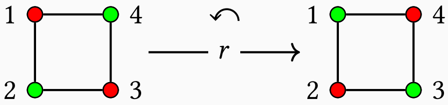
For block Δ, define **block system** $\Sigma = \{\Delta^g : g \in G\}$ (partitions Ω); then G acts on Σ; if Δ is *maximal*, then acts primitively.

Blocks and primitivity (ii)

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 $r = (1,2,3,4)$, $s = (1,4)(2,3)$, $sr = (2,4)$.

Block is $\Delta = \{1,3\}$ (nontrivial) with block system $\Sigma = \{\{1,3\},\{2,4\}\}$ (opposite vertices stay opposite):



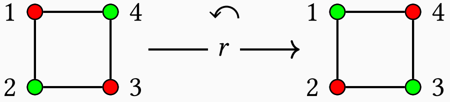
e.g. $\Delta^r = \{2,4\}$,

Blocks and primitivity (ii)

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 $r = (1,2,3,4)$, $s = (1,4)(2,3)$, $sr = (2,4)$.

Block is $\Delta = \{1,3\}$ (nontrivial) with block system $\Sigma = \{\{1,3\},\{2,4\}\}$ (opposite vertices stay opposite):



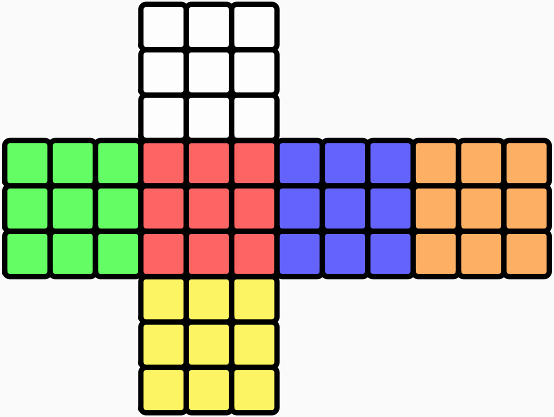
e.g. $\Delta^r = \{2,4\}$, $\Delta^s = \{4,2\}$, $\Delta^{sr} = \{1,3\} = \Delta$.

D_8 acts imprimitively on $[4]$ but primitively on Σ (degree 2).

The Rubik's group

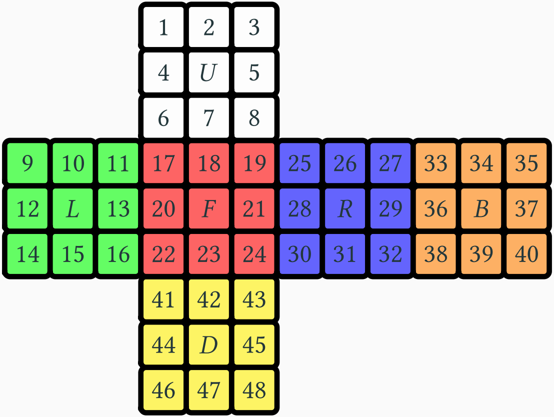
Representing the cube and its operations

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



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

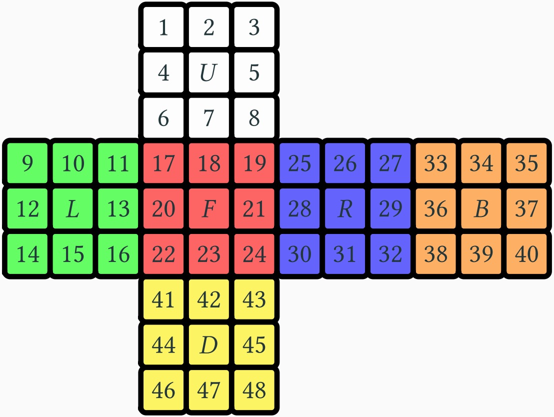
In **solved state** 1, label stickers (except each centre) using $[48]$:



Representing the cube and its operations

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

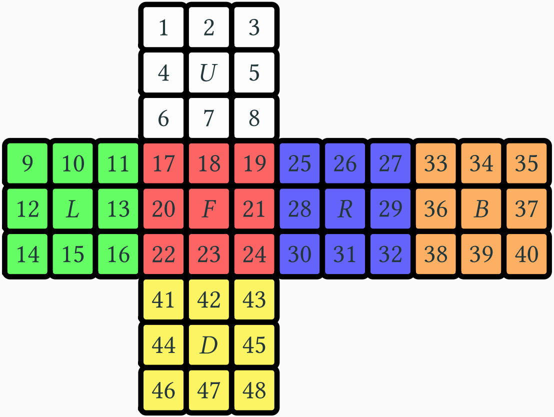
In **solved state** 1, label stickers (except each centre) using $[48]$:



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

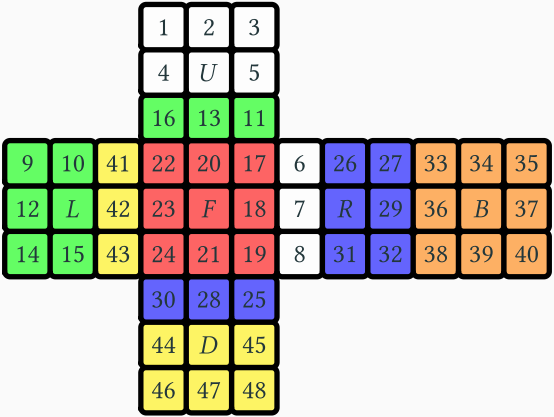
Representing the cube and its operations (ii)

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



Representing the cube and its operations (ii)

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



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

The Rubik's group of permutations

Generators as permutations of labels [48]:

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

The Rubik's group of permutations

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. $RUR^{-1}U^{-1}$,

The Rubik's group of permutations

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. $RUR^{-1}U^{-1}$, $URU^{-1}L^{-1}UR^{-1}U^{-1}L$,

The Rubik's group of permutations

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. $RUR^{-1}U^{-1}$, $URU^{-1}L^{-1}UR^{-1}U^{-1}L$, $RUR^{-1}URU^2R^{-1}U^2$,

The Rubik's group of permutations

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. $RUR^{-1}U^{-1}$, $URU^{-1}L^{-1}UR^{-1}U^{-1}L$, $RUR^{-1}URU^2R^{-1}U^2$, $1 = ()$.

Definition (Rubik's group)

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

Clearly $\mathcal{G}$ is 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 );
```

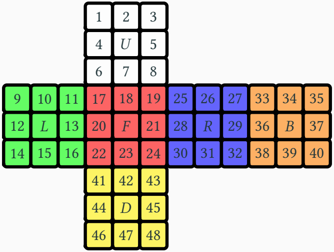
The Rubik's group of permutations (ii)

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?*

Orbits in the Rubik's group

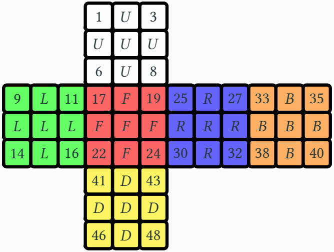



```
gap> Orbit( G, 1 );
[ 1, 6, 40, 27, 8, 35, 16, 41, 32, 25, 48, 3, 11, 24, 46, 33, 43, 17, 30,
      14, 19, 9, 22, 38 ]
gap> Orbit( G, 2 );
[ 2, 5, 12, 7, 36, 10, 47, 4, 28, 45, 34, 13, 29, 44, 20, 42, 26, 21, 37,
      15, 31, 18, 23, 39 ]
```

Two $\mathcal{G}$-orbits: corner stickers $1^{\mathcal{G}}$, edge stickers $2^{\mathcal{G}}$.

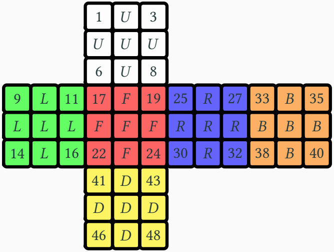
Transitive action on corners

$\mathcal{G}$ acts transitively on corner stickers $1^{\mathcal{G}}$. In this action:



Transitive action on corners

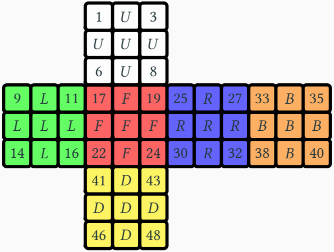
$\mathcal{G}$ acts transitively on corner stickers $1^{\mathcal{G}}$. In this action:



$$\Sigma = \{\overbrace{\{1, 35, 9\}}^{UBL}, \overbrace{\{6, 11, 17\}}^{ULF}, \overbrace{\{40, 46, 14\}}^{BDL}, \overbrace{\{27, 3, 33\}}^{RUB},$$
$$\underbrace{\{8, 25, 19\}}_{URF}, \underbrace{\{16, 41, 22\}}_{LDF}, \underbrace{\{32, 48, 38\}}_{RDB}, \underbrace{\{24, 43, 30\}}_{FDR}\}$$

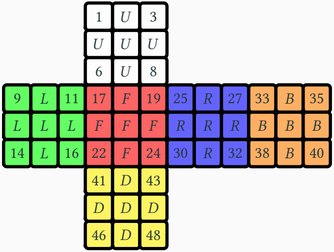
is block system for *maximal* block $\{8, 25, 19\}$ (URF corner).

Transitive action on corners (ii)



$\mathcal{G}$ acts primitively on Σ (degree 8); $g \in \mathcal{G}$ induces perm of Σ, e.g.

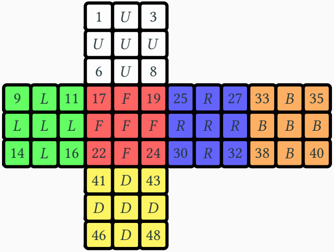
Transitive action on corners (ii)



$\mathcal{G}$ acts primitively on Σ (degree 8); $g \in \mathcal{G}$ induces perm of Σ, e.g.

$$F \mapsto (\underbrace{FUL}_{FDL^F}, \underbrace{FUR}_{FUL^F}, \underbrace{FDR}_{FUR^F}, \underbrace{FDL}_{FDR^F}) \in \mathrm{Sym}(\Sigma).$$

Transitive action on corners (ii)



$\mathcal{G}$ acts primitively on Σ (degree 8); $g \in \mathcal{G}$ induces perm of Σ, e.g.

$$F \mapsto (\underbrace{FUL}_{FDL^F}, \underbrace{FUR}_{FUL^F}, \underbrace{FDR}_{FUR^F}, \underbrace{FDL}_{FDR^F}) \in \mathrm{Sym}(\Sigma).$$

$\mathcal{G}$ induces every perm of Σ (so $\mathrm{Sym}(8)$ "is" *primitive* quotient of $\mathcal{G}$).

Bases and stabiliser chains

Definition (Base, stabiliser chain)

If $G \leq \mathrm{Sym}(\Omega)$, distinct elts $B = [\beta_1, \ldots, \beta_r] \subseteq \Omega$ is **base** for G if $G_{\beta_1,\ldots,\beta_r} = 1$. (*Recall:* $G_{\beta_1,\ldots,\beta_r} = \{g \in G : \beta_1^g = \beta_1, \ldots, \beta_r^g = \beta_r\}$.)

Definition (Base, stabiliser chain)

If $G \leq \mathrm{Sym}(\Omega)$, distinct elts $B = [\beta_1, \ldots, \beta_r] \subseteq \Omega$ is **base** for G if $G_{\beta_1,\ldots,\beta_r} = 1$. (*Recall:* $G_{\beta_1,\ldots,\beta_r} = \{g \in G : \beta_1^g = \beta_1, \ldots, \beta_r^g = \beta_r\}$.)

Corresponding **stabiliser chain** is

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$$

where $G^i = G^{i-1}_{\beta_i} = G_{\beta_1,\ldots,\beta_i}$.

Bases and stabiliser chains

Definition (Base, stabiliser chain)

If $G \leq \mathrm{Sym}(\Omega)$, distinct elts $B = [\beta_1, \ldots, \beta_r] \subseteq \Omega$ is **base** for G if $G_{\beta_1,\ldots,\beta_r} = 1$. (*Recall:* $G_{\beta_1,\ldots,\beta_r} = \{g \in G : \beta_1^g = \beta_1, \ldots, \beta_r^g = \beta_r\}$.)

Corresponding **stabiliser chain** is

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$$

where $G^i = G^{i-1}_{\beta_i} = G_{\beta_1,\ldots,\beta_i}$.

Base B contains elts of Ω such that only $1 \in G$ fixes every $\beta_i \in B$. (Short base desirable: how to compute **min base** of length $b(G)$?)

Definition (Base, stabiliser chain)

If $G \leq \mathrm{Sym}(\Omega)$, distinct elts $B = [\beta_1, \ldots, \beta_r] \subseteq \Omega$ is **base** for G if $G_{\beta_1,\ldots,\beta_r} = 1$. (*Recall:* $G_{\beta_1,\ldots,\beta_r} = \{g \in G : \beta_1^g = \beta_1, \ldots, \beta_r^g = \beta_r\}$.)

Corresponding **stabiliser chain** is

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$$

where $G^i = G^{i-1}_{\beta_i} = G_{\beta_1,\ldots,\beta_i}$.

Base B contains elts of Ω such that only $1 \in G$ fixes every $\beta_i \in B$. (Short base desirable: how to compute **min base** of length $b(G)$?)

Theorem (Blaha, 1992)

Problem of finding minimum base for G is NP-complete, even for cyclic groups (if $\mathrm{P} \neq \mathrm{NP}$, then no polynomial time algorithm).

Bases and stabiliser chains (ii)

Example (Rubik's group)

Using `BaseOfGroup` cmd in `GAP`, base of $\mathcal{G}$ of size 18 is

$$B = [1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21, 23, 24, 29, 31].$$

Bases and stabiliser chains (ii)

Example (Rubik's group)

Using `BaseOfGroup` cmd in `GAP`, base of $\mathcal{G}$ of size 18 is

$$B = [1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21, 23, 24, 29, 31].$$

Contains: 7 corner stickers (from 7 of 8 corners), 11 edge stickers (from 11 of 12 edges).

Bases and stabiliser chains (ii)

Example (Rubik's group)

Using `BaseOfGroup` cmd in `GAP`, base of $\mathcal{G}$ of size 18 is

$$B = [1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21, 23, 24, 29, 31].$$

Contains: 7 corner stickers (from 7 of 8 corners), 11 edge stickers (from 11 of 12 edges).

Theorem

For Rubik's group $\mathcal{G}$, $b(\mathcal{G}) = 18$.

Bases and stabiliser chains (iii)

Stabiliser chain implemented in GAP; useful in algorithms.

Bases and stabiliser chains (iii)

Stabiliser chain implemented in GAP; useful in algorithms.

Let $G = \langle X \rangle \leq \mathrm{Sym}(\Omega)$ have base B and stabiliser chain

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1.$$

Stabiliser chain implemented in GAP; useful in algorithms.

Let $G = \langle X \rangle \leq \mathrm{Sym}(\Omega)$ have base B and stabiliser chain

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1.$$

Problem (random element generation)

Generate uniformly random element of G.

(*Alternative:*

Bases and stabiliser chains (iii)

Stabiliser chain implemented in GAP; useful in algorithms.

Let $G = \langle X \rangle \leq \mathrm{Sym}(\Omega)$ have base B and stabiliser chain

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1.$$

Problem (random element generation)

Generate uniformly random element of G.

(*Alternative:* random product of generators in X; transitive Markov chain on Cayley graph (find mixing time?); distribution?)

Stabiliser chain implemented in GAP; useful in algorithms.

Let $G = \langle X \rangle \leq \mathrm{Sym}(\Omega)$ have base B and stabiliser chain

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1.$$

Problem (random element generation)

Generate uniformly random element of G.

(*Alternative:* random product of generators in X; transitive Markov chain on Cayley graph (find mixing time?); distribution?)

Problem (membership testing)

For $g \in \mathrm{Sym}(\Omega)$, test if $g \in G$.

(*Application*:

Bases and stabiliser chains (iii)

Stabiliser chain implemented in `GAP`; useful in algorithms.

Let $G = \langle X \rangle \leq \mathrm{Sym}(\Omega)$ have base B and stabiliser chain

$$G = G^0 \geq G^1 \geq \cdots \geq G^r = 1.$$

Problem (random element generation)

Generate uniformly random element of G.

(*Alternative:* random product of generators in X; transitive Markov chain on Cayley graph (find mixing time?); distribution?)

Problem (membership testing)

For $g \in \mathrm{Sym}(\Omega)$, test if $g \in G$.

(*Application*: check if restickering of Rubik's cube is valid state.)

Greedy bases

Algorithm (greedy base; Brown, Finkelstein & Purdom, 1989)

Construct base $B = [\beta_1, \ldots, \beta_r]$ for $G \leq \mathrm{Sym}(\Omega)$ by

Greedy bases

Algorithm (greedy base; Brown, Finkelstein & Purdom, 1989)

Construct base $B = [\beta_1, \ldots, \beta_r]$ for $G \leq \mathrm{Sym}(\Omega)$ by choosing $\beta_i \in \Omega$ from largest orbit of G^i ($G^0 = G$), then setting $G^i = G^{i-1}_{\beta_i}$ until $G^r = 1$. Then $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ is stabiliser chain.

Greedy bases

Algorithm (greedy base; Brown, Finkelstein & Purdom, 1989)

Construct base $B = [\beta_1, \ldots, \beta_r]$ for $G \leq \mathrm{Sym}(\Omega)$ by choosing $\beta_i \in \Omega$ from largest orbit of G^i ($G^0 = G$), then setting $G^i = G^{i-1}_{\beta_i}$ until $G^r = 1$. Then $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ is stabiliser chain.

Proposition (Blaha, 1992)

Greedy base algorithm does not necessarily find minimum base, even for cyclic groups.

Greedy bases

Algorithm (greedy base; Brown, Finkelstein & Purdom, 1989)
Construct base $B = [\beta_1, \ldots, \beta_r]$ for $G \leq \mathrm{Sym}(\Omega)$ by choosing $\beta_i \in \Omega$ from largest orbit of G^i ($G^0 = G$), then setting $G^i = G^{i-1}_{\beta_i}$ until $G^r = 1$. Then $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ is stabiliser chain.

Proposition (Blaha, 1992)
Greedy base algorithm does not necessarily find minimum base, even for cyclic groups.

Theorem (Blaha, 1992)
Size of greedy base for $G \leq \mathrm{Sym}(n)$ *is at most* $O(b(G) \log \log n)$.

Greedy bases

Algorithm (greedy base; Brown, Finkelstein & Purdom, 1989)
Construct base $B = [\beta_1, \ldots, \beta_r]$ for $G \leq \mathrm{Sym}(\Omega)$ by choosing $\beta_i \in \Omega$ from largest orbit of G^i ($G^0 = G$), then setting $G^i = G^{i-1}_{\beta_i}$ until $G^r = 1$. Then $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ is stabiliser chain.

Proposition (Blaha, 1992)
Greedy base algorithm does not necessarily find minimum base, even for cyclic groups.

Theorem (Blaha, 1992)
Size of greedy base for $G \leq \mathrm{Sym}(n)$ *is at most* $O(b(G) \log \log n)$.
(Compared to arbitrary nonredundant base, with size $O(b(G) \log n)$*.)*

What is the size of the Rubik's group?

Theorem (size of perm group)

If $B = [\beta_1, \ldots, \beta_r]$ *is base for* $G \leq \mathrm{Sym}(n)$ *with stabiliser chain* $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$, *then*

$$|G| = |\beta_1^{G^0}||\beta_2^{G^1}| \cdots |\beta_r^{G^{r-1}}|.$$

What is the size of the Rubik's group?

Theorem (size of perm group)
If $B = [\beta_1, \ldots, \beta_r]$ *is base for* $G \leq \mathrm{Sym}(n)$ *with stabiliser chain* $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$*, then*

$$|G| = |\beta_1^{G^0}||\beta_2^{G^1}| \cdots |\beta_r^{G^{r-1}}|.$$

Orbits and stabilisers can be easily computed (e.g. using `GAP`).

What is the size of the Rubik's group?

Theorem (size of perm group)
If $B = [\beta_1, \dots, \beta_r]$ is base for $G \leq \mathrm{Sym}(n)$ with stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$, then

$$|G| = |\beta_1^{G^0}||\beta_2^{G^1}| \cdots |\beta_r^{G^{r-1}}|.$$

Orbits and stabilisers can be easily computed (e.g. using `GAP`).

Implementing base and stabiliser chain for Rubik's group $\mathcal{G}$ (using `BaseOfGroup` and `StabChain` cmds), `GAP` computes:

What is the size of the Rubik's group?

Theorem (size of perm group)
If $B = [\beta_1, \ldots, \beta_r]$ *is base for* $G \leq \mathrm{Sym}(n)$ *with stabiliser chain* $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$*, then*

$$|G| = |\beta_1^{G^0}||\beta_2^{G^1}| \cdots |\beta_r^{G^{r-1}}|.$$

Orbits and stabilisers can be easily computed (e.g. using `GAP`).

Implementing base and stabiliser chain for Rubik's group $\mathcal{G}$ (using `BaseOfGroup` and `StabChain` cmds), `GAP` computes:

Corollary
$|\mathcal{G}| = 43\,252\,003\,274\,489\,856\,000 \approx 4.3 \cdot 10^{19}.$

Base sizes of primitive groups

Affine groups

Definition

Let K be field. **Affine transformation** of K^d is map

$$t_{a,v} : K^d \to K^d, \quad u \mapsto ua + v$$

for $a \in \mathrm{GL}_d(K)$ and $v \in K^d$. (Treat u, v as row vectors.)

Definition

Let K be field. **Affine transformation** of K^d is map

$$t_{a,v} : K^d \to K^d, \quad u \mapsto ua + v$$

for $a \in \mathrm{GL}_d(K)$ and $v \in K^d$. (Treat u, v as row vectors.)

Note: $t_{a,v} \in \mathrm{Sym}(K^d)$ (bijection).

Affine groups

Definition

Let K be field. **Affine transformation** of K^d is map

$$t_{a,v} : K^d \to K^d, \quad u \mapsto ua + v$$

for $a \in \mathrm{GL}_d(K)$ and $v \in K^d$. (Treat u, v as row vectors.)

Note: $t_{a,v} \in \mathrm{Sym}(K^d)$ (bijection).

Definition

Affine group $\mathrm{AGL}_d(K) \leq \mathrm{Sym}(K^d)$ of dim d is affine transfs of K^d.
For $K = \mathbb{F}_q$ finite field, write $\mathrm{AGL}_d(q)$ (perm group of deg q^d).

Affine groups

Definition

Let K be field. **Affine transformation** of K^d is map

$$t_{a,v} : K^d \to K^d, \quad u \mapsto ua + v$$

for $a \in \mathrm{GL}_d(K)$ and $v \in K^d$. (Treat u, v as row vectors.)

Note: $t_{a,v} \in \mathrm{Sym}(K^d)$ (bijection).

Definition

Affine group $\mathrm{AGL}_d(K) \leq \mathrm{Sym}(K^d)$ of dim d is affine transfs of K^d.
For $K = \mathbb{F}_q$ finite field, write $\mathrm{AGL}_d(q)$ (perm group of deg q^d).

Interested in $q = 2$, i.e. field $\mathbb{F}_2 = \{0, 1\}$ with $1 + 1 = 0$, $1 \cdot 1 = 1$, etc.

Definition

Perm group G of degree n is **large base** if

$$\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$$

for some m, r, k, where $\mathrm{Sym}(m)$ acts on $\binom{[m]}{k}$ and $n = \binom{m}{k}^r$.

Definition

Perm group G of degree n is **large base** if

$$\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$$

for some m, r, k, where $\mathrm{Sym}(m)$ acts on $\binom{[m]}{k}$ and $n = \binom{m}{k}^r$.

Theorem (Liebeck, 1984)

For primitive perm group G of degree n, either:

(i) *G is large base; or*

(ii) *$b(G) < 9 \log n$.*

Large base permutation groups

Definition

Perm group G of degree n is **large base** if

$$\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$$

for some m, r, k, where $\mathrm{Sym}(m)$ acts on $\binom{[m]}{k}$ and $n = \binom{m}{k}^r$.

Theorem (Liebeck, 1984)

For primitive perm group G of degree n, either:

(i) *G is large base; or*

(ii) $b(G) < 9 \log n$.

"Remarkable" proof used *classification of finite simple groups*, *O'Nan-Scott theorem* (classifies primitive groups).

Large base permutation groups (ii)

Theorem (Moscatiello & Roney-Dougal, 2021)

For primitive perm group G of degree n, and G is non-large base:

(i) *G is the Mathieu group M_{24} (degree 24); or*

(ii) $b(G) \leq \lceil \log n \rceil + 1$.

Large base permutation groups (ii)

Theorem (Moscatiello & Roney-Dougal, 2021)
For primitive perm group G of degree n, and G is non-large base:

(i) *G is the Mathieu group M_{24} (degree 24); or*

(ii) $b(G) \leq \lceil \log n \rceil + 1$.

Moreover, if $b(G) = \log n + 1$ then $G \leq \mathrm{AGL}_d(2)$ with $n = 2^d$.

Large base permutation groups (ii)

Theorem (Moscatiello & Roney-Dougal, 2021)

For primitive perm group G of degree n, and G is non-large base:

(i) *G is the Mathieu group M_{24} (degree 24); or*

(ii) $b(G) \leq \lceil \log n \rceil + 1$.

Moreover, if $b(G) = \log n + 1$ then $G \leq \mathrm{AGL}_d(2)$ with $n = 2^d$.

Question (Moscatiello & Roney-Dougal, 2021)

Which primitive groups $G \leq \mathrm{Sym}(n)$ satisfy $b(G) = \log n + 1$?

Theorem

Let $G \leq \mathrm{AGL}_d(2)$ *be primitive for some* d *with natural action on* K^d *with* $b(G) = d + 1$. *(Then* G *is perm group of degree* $n = 2^d$.*)*

(i) *For* $d = 1$, *there is no such* G.

Theorem

Let $G \leq \mathrm{AGL}_d(2)$ *be primitive for some* d *with natural action on* K^d *with* $b(G) = d + 1$. *(Then* G *is perm group of degree* $n = 2^d$.*)*

(i) *For* $d = 1$, *there is no such* G.

(ii) *For odd* $3 \leq d \leq 9$ *and* $d = 2$, *then* G *is* $\mathrm{AGL}_d(2)$.

Main result in thesis

Theorem

Let $G \leq \mathrm{AGL}_d(2)$ be primitive for some d with natural action on K^d with $b(G) = d + 1$. (Then G is perm group of degree $n = 2^d$.)

(i) *For $d = 1$, there is no such G.*

(ii) *For odd $3 \leq d \leq 9$ and $d = 2$, then G is $\mathrm{AGL}_d(2)$.*

(iii) *For even $4 \leq d \leq 10$, then G is $\mathrm{AGL}_d(2)$ or $2^d : \mathrm{Sp}_d(2)$.*

Proof (idea).

- Find representatives M of conjugacy classes of primitive maximal subgroups of $\mathrm{AGL}_d(2)$.

Proof (idea).

- Find representatives M of conjugacy classes of primitive maximal subgroups of $\mathrm{AGL}_d(2)$.
- Use greedy base algorithm to find base for M; if base of length at most d is found then $b(M) \leq d$ and discard.

Main result in thesis (ii)

Proof (idea).

- Find representatives M of conjugacy classes of primitive maximal subgroups of $\mathrm{AGL}_d(2)$.
- Use greedy base algorithm to find base for M; if base of length at most d is found then $b(M) \leq d$ and discard.
- Otherwise, recursively check for each representative M.

Proof (idea).

- Find representatives M of conjugacy classes of primitive maximal subgroups of $\mathrm{AGL}_d(2)$.
- Use greedy base algorithm to find base for M; if base of length at most d is found then $b(M) \leq d$ and discard.
- Otherwise, recursively check for each representative M.

Every primitive $G \leq \mathrm{AGL}_d(2)$ with $b(G) = d + 1$ is found by process (plus perhaps false positives), up to conjugacy. $\square$

Greedy base algorithm performed better than `BaseOfGroup` in testing; found no false positives.

Main result in thesis (iii)

From above theorem, we conjecture the following:

Conjecture

Primitive group $G \leq \mathrm{Sym}(n)$ satisfies $b(G) = \log n + 1$ iff:

Main result in thesis (iii)

From above theorem, we conjecture the following:

Conjecture

Primitive group $G \leq \mathrm{Sym}(n)$ satisfies $b(G) = \log n + 1$ iff:

- $n = 2^d$ with $d \geq 2$, and G is $\mathrm{AGL}_d(2)$; or
- $n = 2^d$ with $d \geq 4$, and G is $2^d : \mathrm{Sp}_d(2)$.

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)
- Blaha — *Minimum bases for permutation groups: The greedy approximation*, 1992: https://doi:10.1016/0196-6774(92)90020-D
- Liebeck — *On minimal degrees and base sizes of primitive permutation groups*, 1984: https://doi.org/10.1007/bf01193603
- Moscatiello and Roney-Dougal: *Base sizes of primitive permutation groups*, 2021: https://doi.org/10.1007/s00605-021-01599-5