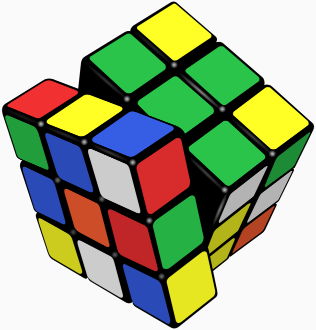
Rubik’s cubes and permutation group theory

Lawrence Chen

October 8, 2022

Honours presentation



Contents

Some basic group theory

- What is a group?
- Order and generators
- Permutations
- Group actions

The Rubik's group

- Representing the cube and its moves
- Moves vs states for Rubik's cube
- The Rubik's group of permutations
- Orbits and stabilisers
- Orders of moves
- Jake's theorems

Analysing the Rubik's group

- Bases and stabiliser chains
- How many valid states are there?
- Can this restickering be solved?
- Solving a Rubik's cube...

Concluding remarks

- References

Questions about Rubik's cube i

- How can we represent *move sequences* and *states* of a cube?

Questions about Rubik's cube i

- How can we represent *move sequences* and *states* of a cube?
- How can we tell *how many* states a Rubik's cube can take?

Questions about Rubik's cube i

- 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*?

Questions about Rubik's cube i

- 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*?

Questions about Rubik's cube i

- 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?

Questions about Rubik's cube i

- 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?

Answer: using permutations and *permutation group theory*!

- 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?

Answer: using permutations and *permutation 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

What is a group? i

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh,$

What is a group? i

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

Example (Integers under addition)

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

Example (Integers under addition)

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses

What is a group? i

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

Example (Integers under addition)

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

What is a group? i

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

Example (Integers under addition)

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

Example (Cyclic group)

The set $C_n = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ with rules $a^k a^\ell = a^{k+\ell}$, $a^n = a^0$ forms group: identity

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

Example (Integers under addition)

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

Example (Cyclic group)

The set $C_n = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ with rules $a^k a^\ell = a^{k+\ell}$, $a^n = a^0$ forms group: identity $1 = a^0$, inverses

Definition (group)

A **group** is a set $G \neq \emptyset$ with operation $G \times G \to G,\ (g, h) \mapsto gh$,

(i) **(identity)** there is $1 \in G$ with $1g = g1 = g$ for all $g \in G$;

(ii) **(inverses)** for all $g \in G$, there is $g^{-1} \in G$ with $g^{-1}g = gg^{-1} = 1$;

(iii) **(associative)** $(gh)k = g(hk)$ for all $g, h, k \in G$.

Example (Integers under addition)

The integers $(\mathbb{Z}, +)$ form an **abelian** group: identity 0, inverses $-k$ for $k \in \mathbb{Z}$, associative.

Example (Cyclic group)

The set $C_n = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ with rules $a^k a^\ell = a^{k+\ell}$, $a^n = a^0$ forms group: identity $1 = a^0$, inverses a^{-k} for $a^k \in C_n$, associative.

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is 4.

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is 4.

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 $G = \langle X \rangle$.

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is 4.

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 $|X| = 1$, G is **cyclic**.)

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is 4.

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 $|X| = 1$, G is **cyclic**.)

Example (Cyclic group)

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$:

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is 4.

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 $|X| = 1$, G is **cyclic**.)

Example (Cyclic group)

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$: $C_6 = \langle a \rangle$.

Order and generators i

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is 4.

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 $|X| = 1$, G is **cyclic**.)

Example (Cyclic group)

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$: $C_6 = \langle a \rangle$. If $b = a^2$, $c = a^3$ then $C_6 = \langle b, c \rangle$ since

Definition (order)

Order of $g \in G$ is least $k \in \mathbb{Z}_+$ with $g^k = g \cdots g = 1$ (otherwise ∞).

Example (Cyclic group)

Consider group $C_4 = \{1, a, a^2, a^3\}$: order of 1 is 1, order of a is 4, order of a^2 is 2, order of a^3 is 4.

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 $|X| = 1$, G is **cyclic**.)

Example (Cyclic group)

Consider group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$: $C_6 = \langle a \rangle$. If $b = a^2$, $c = a^3$ then $C_6 = \langle b, c \rangle$ since $a = cb^{-1}$ so $a^k = cb^{-1} \cdots cb^{-1} = c^k b^{-k}$.

Definition (permutation)

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

Permutations i

Definition (permutation)

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

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

Permutations i

Definition (permutation)

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

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 i

Definition (permutation)

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

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:

$$\begin{tikzcd}
 & 1 \arrow[ddrrr] & 2 & 3 & 4 & 5 & 6 \\
\sigma & & & & & & \\
 & 1 & 2 & 3 & 4 & 5 & 6
\end{tikzcd}$$

It means

$$1^\sigma = 4,$$

Definition (permutation)

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

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:

$$\begin{tikzcd}
 & 1 \arrow[ddrrr] & 2 & 3 & 4 \arrow[ddr] & 5 & 6 \\
\sigma & & & & & & \\
 & 1 & 2 & 3 & 4 & 5 & 6
\end{tikzcd}$$

It means

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

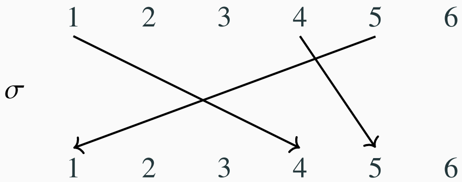
Permutations i

Definition (permutation)

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

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

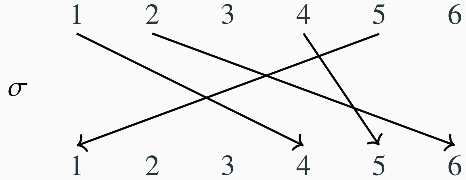
$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,$$

Definition (permutation)

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

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

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

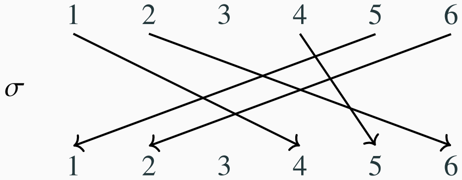
Permutations i

Definition (permutation)

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

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

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

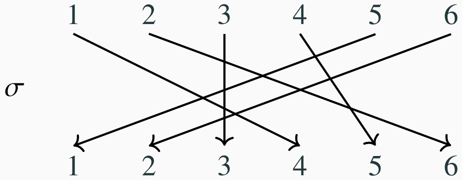
Permutations i

Definition (permutation)

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

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

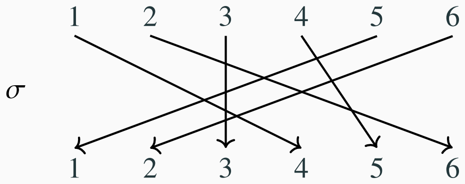
Cycle notation: $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$ is:



It means

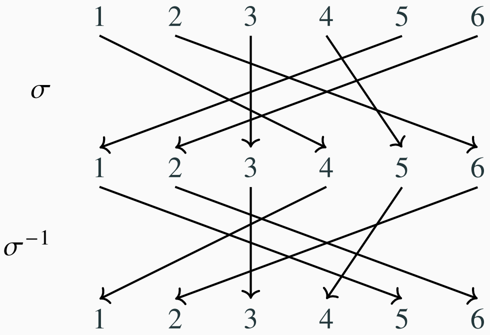
$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,\ 6^\sigma = 2,\ 3^\sigma = 3.$$

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



Permutations ii

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

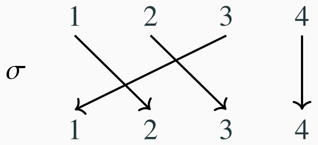


Inverse is $\sigma^{-1} = (1,5,4)(2,6) \in \mathrm{Sym}(6)$.

Permutations iii

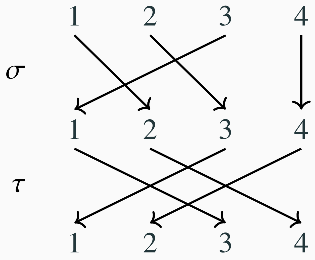
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first σ, then τ”, so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$.

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



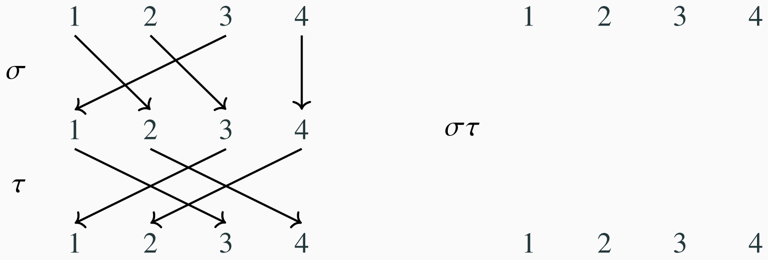
Permutations iii

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



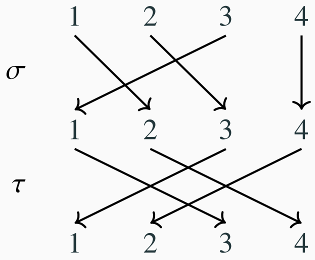
Permutations iii

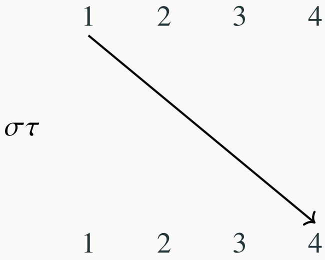
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,



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

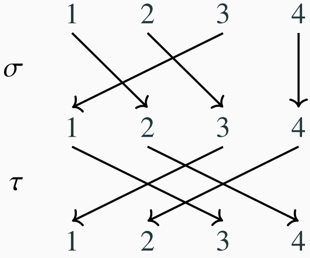
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^\sigma)^\tau$. E.g. $\sigma = (1,2,3), \tau = (1,3)(2,4) \in \mathrm{Sym}(4)$,

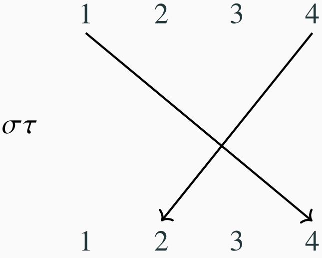




$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,$$

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

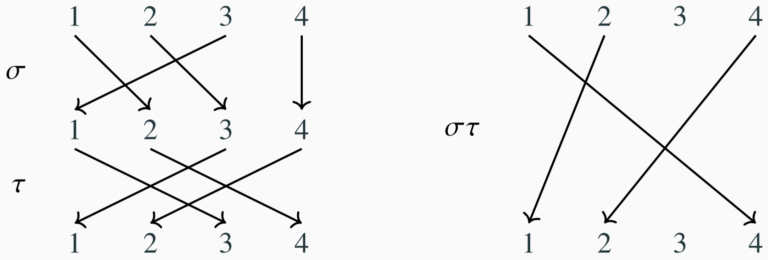




$$\sigma\tau = (1, 2, 3)(1, 3)(2, 4) = (1, 4, 2$$

Permutations iii

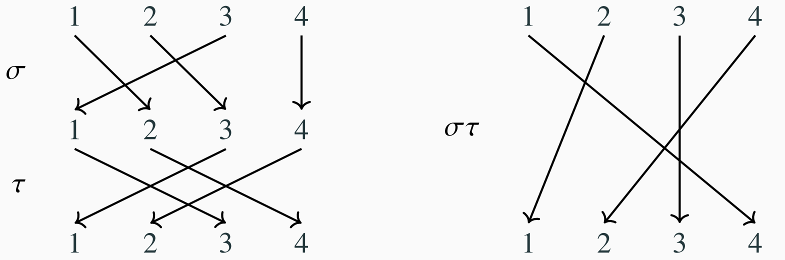
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means “first σ, then τ”, so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3), \tau = (1, 3)(2, 4) \in \mathrm{Sym}(4)$,



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

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



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

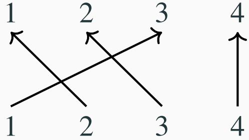
Permutations iv

Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

$\sigma^{-1} = (1, 3, 2)$,

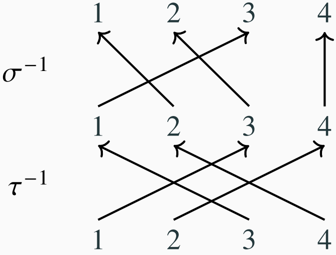
σ^{-1}



Permutations iv

Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

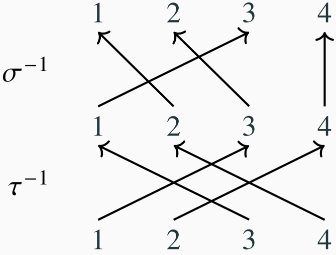
$\sigma^{-1} = (1, 3, 2)$, $\tau^{-1} = (1, 3)(2, 4)$,

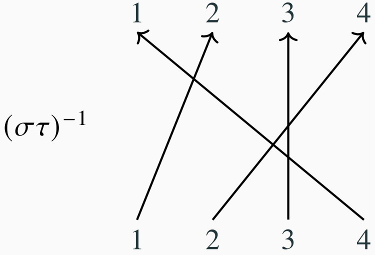


Permutations iv

Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

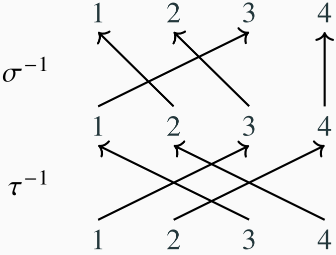
$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$, $(\sigma\tau)^{-1} = (1,2,4)$.

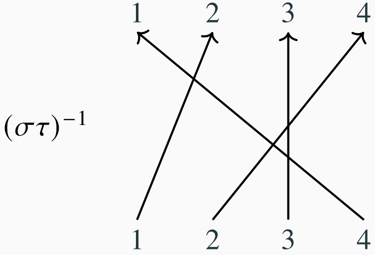




Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$, $(\sigma\tau)^{-1} = (1,2,4)$.



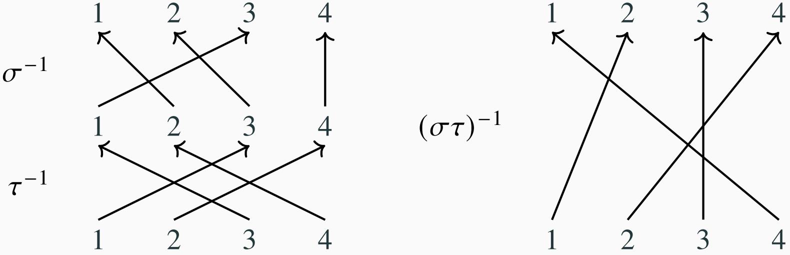


$$\sigma^{-1}\tau^{-1} = (1,3,2)(1,3)(2,4) = (2,3,4) \neq (\sigma\tau)^{-1},$$

Permutations iv

Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$, $(\sigma\tau)^{-1} = (1,2,4)$.



$$\sigma^{-1}\tau^{-1} = (1,3,2)(1,3)(2,4) = (2,3,4) \neq (\sigma\tau)^{-1},$$
$$\tau^{-1}\sigma^{-1} = (1,3)(2,4)(1,3,2) = (1,2,4) = (\sigma\tau)^{-1}.$$

Permutations v

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$?

Permutations v

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? *Answer:* $n!$

Example (Order of permutation)

Consider $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$. Then $1^{\sigma^3} = 4^{\sigma^2} = 5^{\sigma} = 1$,

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? *Answer:* $n!$

Example (Order of permutation)

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

Permutations v

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? *Answer:* $n!$

Example (Order of permutation)

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.

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? *Answer:* $n!$

Example (Order of permutation)

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.

Fact: order of $\sigma \in \mathrm{Sym}(n)$ is lcm of cycle lengths.

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? *Answer:* $n!$

Example (Order of permutation)

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.

Fact: order of $\sigma \in \mathrm{Sym}(n)$ is lcm of cycle lengths.

Definition (subgroup)

Subset H of group G is **subgroup** if it is group under same operation; write $H \leq G$. (Need to check: nonempty, closure, inverses.)

Set of permutations under *product* is **symmetric group** $\mathrm{Sym}(n)$: identity $1 = ()$, inverses (since bijection), associative.

What is size of $\mathrm{Sym}(n)$? *Answer:* $n!$

Example (Order of permutation)

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.

Fact: order of $\sigma \in \mathrm{Sym}(n)$ is lcm of cycle lengths.

Definition (subgroup)

Subset H of group G is **subgroup** if it is group under same operation; write $H \leq G$. (Need to check: nonempty, closure, inverses.)

Definition (permutation group)

A **permutation group** of *degree* n is a subgroup of $\mathrm{Sym}(n)$.

Definition (group action)

If G is group and $\Omega \neq \emptyset$ is set, a G**-action** is a 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 $g, h \in G$.

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

Group actions i

Definition (group action)

If G is group and $\Omega \neq \emptyset$ is set, a G**-action** is a 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 $g, h \in G$.

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

Example (adding time)

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

Group actions i

Definition (group action)

If G is group and $\Omega \neq \emptyset$ is set, a G**-action** is a 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 $g, h \in G$.

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

Example (adding time)

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

E.g. 5:00 plus 9 hrs is $(5{:}00)^9 = [5 + 9]_{12}{:}00 = 2{:}00$.

Definition (group action)

If G is group and $\Omega \neq \emptyset$ is set, a G**-action** is a 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 $g, h \in G$.

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

Example (adding time)

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

E.g. 5:00 plus 9 hrs is $(5{:}00)^9 = [5 + 9]_{12}{:}00 = 2{:}00$.

Example (natural action)

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

Group actions i

Definition (group action)

If G is group and $\Omega \neq \emptyset$ is set, a G**-action** is a 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 $g, h \in G$.

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

Example (adding time)

$\mathbb{Z}$ acts on $\Omega = \{12{:}00, 1{:}00, \ldots, 11{:}00\}$ by $(\alpha{:}00)^k = [\alpha + k]_{12}{:}00$ for $\alpha{:}00 \in \Omega$ and $k \in \mathbb{Z}$.

E.g. 5:00 plus 9 hrs is $(5{:}00)^9 = [5+9]_{12}{:}00 = 2{:}00$.

Example (natural action)

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

Example (right regular action)

Group G acts on $\Omega = G$ (itself) via $\alpha^g = \alpha g$ for $\alpha, g \in G$.

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 $g \in G$.

Group actions ii

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 $\alpha \in \Omega$.

Group actions ii

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 (Adding time)

$\mathbb{Z}$-orbit of 11:00 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 (Adding time)

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).

$\mathbb{Z}$-stabiliser of 11:00 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 (Adding time)

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

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 (Adding time)

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

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

Group actions ii

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 (Adding time)

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \dots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

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

Group actions ii

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 (Adding time)

$\mathbb{Z}$-orbit of 11:00 is $\Omega = \{12{:}00, \ldots, 11{:}00\}$ (e.g. $(11{:}00)^{-2} = 9{:}00$).
$\mathbb{Z}$-stabiliser of 11:00 is $12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ (add multiples of 12 hrs).

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

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

Group actions iii

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

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

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 $G_3 = G$.

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: $|1^G||G_1| = 3 \cdot 1 = 3$

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

Group actions iii

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)

$G = \{(), (1,2,4), (1,4,2)\} \le \mathrm{Sym}(4)$ 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: $|1^G||G_1| = 3 \cdot 1 = 3 = |G|$, $|3^G||G_3| = 1 \cdot 3 = 3 = |G|$.

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

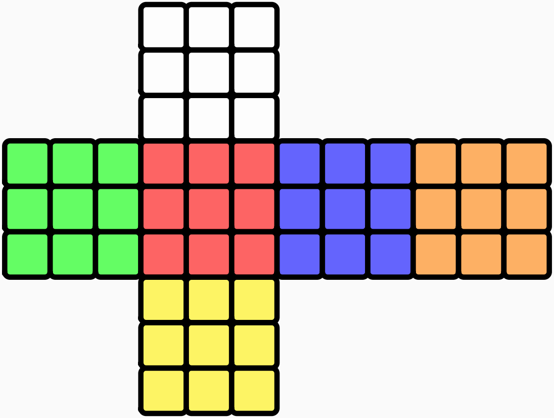
Theorem (orbit-stabiliser)

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

The Rubik's group

Representing the cube and its moves i

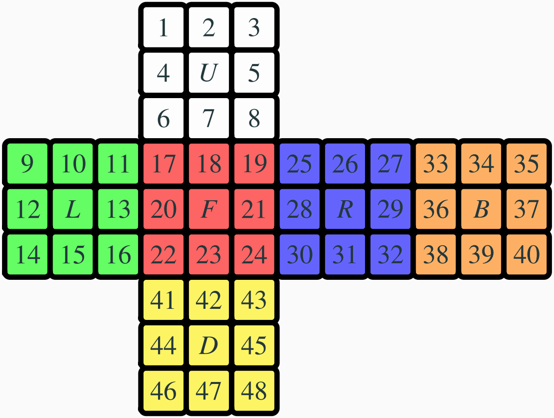
A Rubik's cube has 6 large faces (each with 3×3 smaller faces).



Representing the cube and its moves i

A Rubik's cube has 6 large faces (each with 3×3 smaller faces).

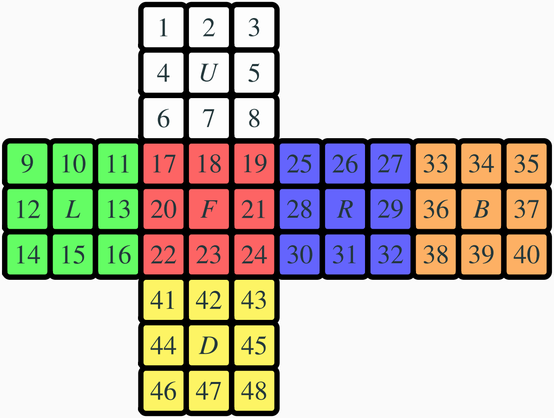
In **solved state** 1, label smaller faces (except each centre) using $[48]$:



Representing the cube and its moves i

A Rubik's cube has 6 large faces (each with 3×3 smaller faces).

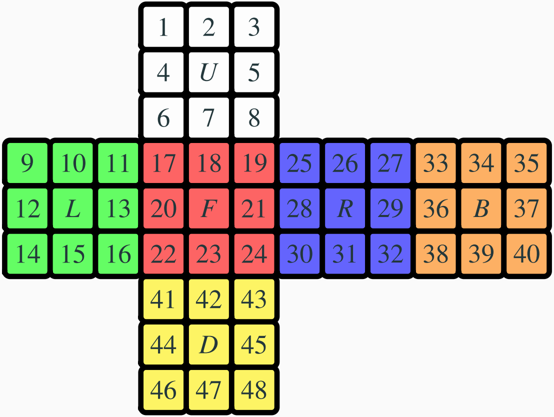
In **solved state** 1, label smaller faces (except each centre) using $[48]$:



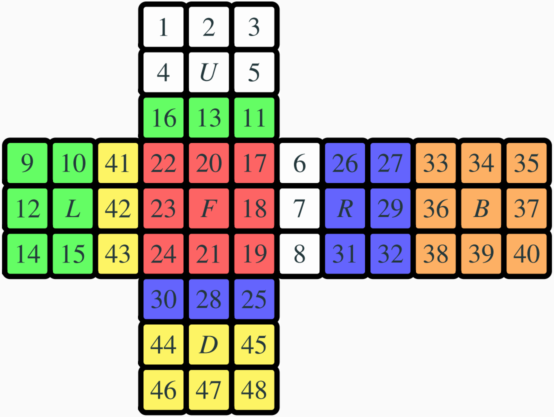
6 **generators** (*moves* in CC): U, L, F, R, B, D (rot. *clockwise*).

Representing the cube and its moves ii

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



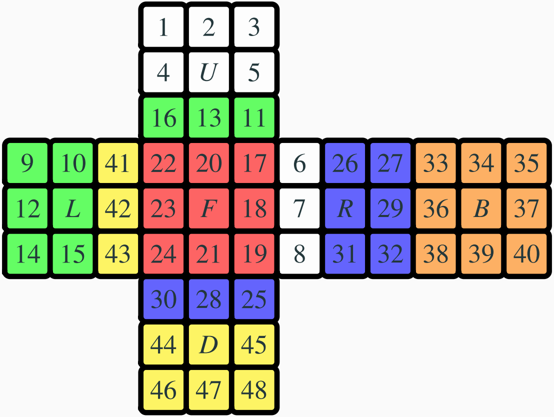
From *solved state* 1, consider F which rotates front face clockwise:



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

Representing the cube and its moves ii

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



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]:

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

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

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

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: $1 = RR^{-1}$).

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*. Generators called *moves*. *Inverse generators* written U', L', F', R', B', D' (instead of U^{-1} etc.); powers written $U2$, $R2$ etc. (instead of U^2, R^2).

Representing the cube and its moves iv

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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 $i \in [n]$.

Representing the cube and its moves iv

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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

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

$19^{RU} =$

Representing the cube and its moves iv

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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

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

$$19^{RU} = (19^R)^U =$$

Representing the cube and its moves iv

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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

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

$$19^{RU} = (19^R)^U = 3^U =$$

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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

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

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

Representing the cube and its moves iv

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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

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

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

Representing the cube and its moves iv

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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

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

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

Representing the cube and its moves iv

In cubing community: moves called *move sequences*. Generators called *moves*. *Inverse generators* 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 $i \in [n]$.

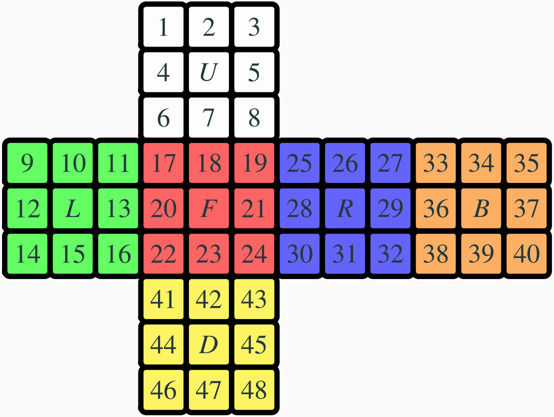
Moves *don't generally commute*: $RU \neq UR$ since

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

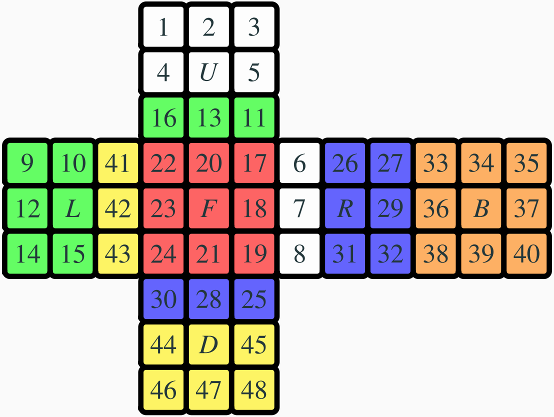
$$19^{RU} = (19^R)^U = 3^U = 8 \quad \text{but} \quad 19^{UR} = (19^U)^R = 11^R = 11.$$

Moves vs states for Rubik's cube i

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



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



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 label at x-position of i in solved state 1.)

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 Sym(48) giving permutation of labels to solved state $1 \in \mathcal{S}$.
(I.e. i^x is label at x-position of i in solved state 1.)

Let $\mathcal{G}$ be valid **moves**; let move $\sigma \in \mathcal{G}$ be element of Sym(48) giving corresponding permutation of labels.
(I.e. i^σ is label at position σ maps i into.)

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 Sym(48) giving permutation of labels to solved state $1 \in \mathcal{S}$.
(I.e. i^x is label at x-position of i in solved state 1.)

Let $\mathcal{G}$ be valid **moves**; let move $\sigma \in \mathcal{G}$ be element of Sym(48) giving corresponding permutation of labels.
(I.e. i^σ is label at position σ maps i into.)

- State $x \in \mathcal{S}$ corresponds to move $x \in \mathcal{G}$ required to get solved state 1 into state x.

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 label at x-position of i in solved state 1.)

Let $\mathcal{G}$ be valid **moves**; let move $\sigma \in \mathcal{G}$ be element of $\mathrm{Sym}(48)$ giving corresponding permutation of labels.
(I.e. i^σ is label at position σ maps i into.)

- 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.

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 Sym(48) giving permutation of labels to solved state $1 \in \mathcal{S}$.
(I.e. i^x is label at x-position of i in solved state 1.)

Let $\mathcal{G}$ be valid **moves**; let move $\sigma \in \mathcal{G}$ be element of Sym(48) giving corresponding permutation of labels.
(I.e. i^σ is label at position σ maps i into.)

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

Set of moves $\mathcal{G}$ forms group: composition of valid moves

The Rubik's group of permutations i

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move is

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move is $1 = () \in \mathcal{G}$, inverse moves

The Rubik's group of permutations i

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move is $1 = () \in \mathcal{G}$, inverse moves exist (undo generators/inverses); associative.

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move is $1 = () \in \mathcal{G}$, inverse moves exist (undo generators/inverses); associative.

Definition (Rubik's group)
$\mathcal{G} \leq \mathrm{Sym}(48)$ is permutation group of degree 48, called the **Rubik's group**; it acts naturally on $[48]$.

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move is $1 = () \in \mathcal{G}$, inverse moves exist (undo generators/inverses); associative.

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

The Rubik's group of permutations i

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move is $1 = () \in \mathcal{G}$, inverse moves exist (undo generators/inverses); associative.

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

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 $x \in \mathcal{G}$.)

Set of moves $\mathcal{G}$ forms group: composition of valid moves is valid move; identity move is $1 = () \in \mathcal{G}$, inverse moves exist (undo generators/inverses); associative.

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

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 $\leftrightarrow$ 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 );
```

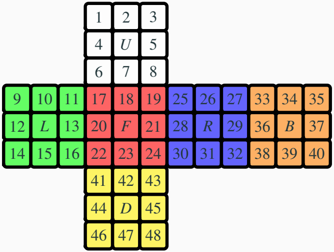
The Rubik's group of permutations ii

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?*

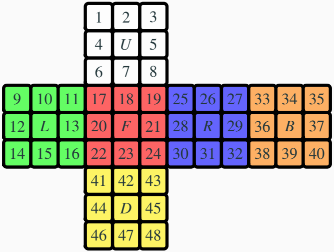
Orbits and stabilisers i




```
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 ]
```

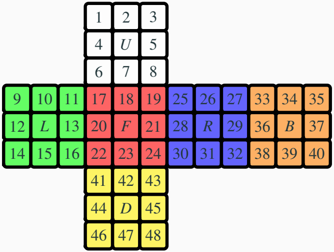
Two $\mathcal{G}$-orbits: corner pieces $1^{\mathcal{G}}$, edge pieces $2^{\mathcal{G}}$.

Orbits and stabilisers i



Moves in $\mathcal{H} = \mathcal{G}_{1,3,6,8} = (((\mathcal{G}_1)_3)_6)_8$ fix white corners $1, 3, 6, 8$.

Orbits and stabilisers i



Moves in $\mathcal{H} = \mathcal{G}_{1,3,6,8} = (((\mathcal{G}_1)_3)_6)_8$ fix white corners 1, 3, 6, 8.

```
gap> G_1368 := Stabilizer( G, [ 1, 3, 6, 8 ], OnTuples );
<permutation group of size 317842469683200 with 12 generators>
gap> Orbit( G_1368, 17 );
[ 17 ]
gap> Orbit( G_1368, 24 );
[ 24, 30, 43, 32, 38, 46, 48, 40, 14, 41, 16, 22 ]
gap> Set( Orbit( G_1368, 2 ) ) = Set( Orbit( G, 2 ) );
true
```

Some $\mathcal{H}$-orbits: $17^{\mathcal{H}} = \{17\}$, bottom corner pieces $24^{\mathcal{H}}$, edge pieces $2^{\mathcal{H}} = 2^{\mathcal{G}}$.

Orders of moves i

Use GAP to compute products, order (using `Order` cmd).

```
gap> R*U*R^(-1)*U^(-1);
(1,27,35,33,9,3)(2,21,5)(8,30,25,43,19,24)(26,34,28)
gap> Order( last );
6
```

How many times must we repeat move $\sigma \in \mathcal{G}$ to have no effect?

Orders of moves i

Use `GAP` to compute products, order (using `Order` cmd).

```
gap> R*U*R^(-1)*U^(-1);
(1,27,35,33,9,3)(2,21,5)(8,30,25,43,19,24)(26,34,28)
gap> Order( last );
6
```

How many times must we repeat move $\sigma \in \mathcal{G}$ to have no effect? I.e. for state $x \in \mathcal{S}$, smallest $k \in \mathbb{Z}_+$ with $x^{\sigma^k} = x\sigma^k = x \iff \sigma^k = 1$.

Orders of moves i

Use GAP to compute products, order (using Order cmd).

```
gap> R*U*R^(-1)*U^(-1);
(1,27,35,33,9,3)(2,21,5)(8,30,25,43,19,24)(26,34,28)
gap> Order( last );
6
```

How many times must we repeat move $\sigma \in \mathcal{G}$ to have no effect? I.e. for state $x \in \mathcal{S}$, smallest $k \in \mathbb{Z}_+$ with $x^{\sigma^k} = x\sigma^k = x \iff \sigma^k = 1$.

Recall: order of σ is lcm of cycle lengths.

- Any *generator* (U, L, F, R, B, D) has cycles of length $4, 4, 4, 4, 4$: order is $\operatorname{lcm}(4, 4, 4, 4, 4) = 4$.

Orders of moves i

Use GAP to compute products, order (using `Order` cmd).

```
gap> R*U*R^(-1)*U^(-1);
(1,27,35,33,9,3)(2,21,5)(8,30,25,43,19,24)(26,34,28)
gap> Order( last );
6
```

How many times must we repeat move $\sigma \in \mathcal{G}$ to have no effect? I.e. for state $x \in \mathcal{S}$, smallest $k \in \mathbb{Z}_+$ with $x^{\sigma^k} = x\sigma^k = x \iff \sigma^k = 1$.

Recall: order of σ is lcm of cycle lengths.

- Any *generator* (U, L, F, R, B, D) has cycles of length $4, 4, 4, 4, 4$: order is $\text{lcm}(4, 4, 4, 4, 4) = 4$.
- *Commutator* $RUR^{-1}U^{-1}$

  $$= (1, 27, 35, 33, 9, 3)(2, 21, 5)(8, 30, 25, 43, 19, 24)(26, 34, 28):$$

  order is $\text{lcm}(6, 3, 6, 3) = 6$.

Orders of moves ii

- *Sune* $RUR^{-1}URU^2R^{-1}U^2$

$$= (1, 9, 35)(2, 5, 7)(3, 33, 27)(8, 25, 19)(18, 34, 26):$$

order is $\mathrm{lcm}(3, 3, 3, 3, 3) = 3$.

Orders of moves ii

- *Sune* $RUR^{-1}URU^2R^{-1}U^2$

$$= (1,9,35)(2,5,7)(3,33,27)(8,25,19)(18,34,26):$$

  order is $\mathrm{lcm}(3,3,3,3,3) = 3$.
- *Lawrence's move* RU has cycles of length $15,7,3,7$: order is $\mathrm{lcm}(15,7,3,7) = 105$.

Orders of moves ii

- *Sune* $RUR^{-1}URU^2R^{-1}U^2$

$$= (1,9,35)(2,5,7)(3,33,27)(8,25,19)(18,34,26):$$

  order is $\operatorname{lcm}(3,3,3,3,3) = 3$.
- *Lawrence's move RU* has cycles of length $15, 7, 3, 7$: order is $\operatorname{lcm}(15,7,3,7) = 105$.
- *Clayton's move* UL' has cycles of length $9, 7, 9, 7$: order is $\operatorname{lcm}(9,7,9,7) = 63$.

Watch video demonstration by my friend Wes :D

Orders of moves ii

- *Sune* $RUR^{-1}URU^2R^{-1}U^2$

$$= (1, 9, 35)(2, 5, 7)(3, 33, 27)(8, 25, 19)(18, 34, 26):$$

  order is $\text{lcm}(3, 3, 3, 3, 3) = 3$.
- *Lawrence's move RU* has cycles of length $15, 7, 3, 7$: order is $\text{lcm}(15, 7, 3, 7) = 105$.
- *Clayton's move* UL' has cycles of length $9, 7, 9, 7$: order is $\text{lcm}(9, 7, 9, 7) = 63$.

Watch video demonstration by my friend Wes :D

Move of order 5?

Orders of moves ii

- *Sune* $RUR^{-1}URU^2R^{-1}U^2$

$$= (1,9,35)(2,5,7)(3,33,27)(8,25,19)(18,34,26):$$

  order is $\mathrm{lcm}(3,3,3,3,3) = 3$.
- *Lawrence's move* RU has cycles of length $15, 7, 3, 7$: order is $\mathrm{lcm}(15,7,3,7) = 105$.
- *Clayton's move* UL' has cycles of length $9, 7, 9, 7$: order is $\mathrm{lcm}(9,7,9,7) = 63$.

Watch video demonstration by my friend Wes :D

Move of order 5? *Answer:* $(RU)^{21}$ since $((RU)^{21})^5 = (RU)^{105} = 1$.

What is smallest $k \in \mathbb{Z}_+$ with no move of that order?

Theorem (Jake Vandenberg's conjecture)

There is no Rubik's cube move that cycles through all states.

Theorem (Jake Vandenberg's conjecture)
There is no Rubik's cube move that cycles through all states.

Recall: states $\leftrightarrow$ moves. Rubik's group $\mathcal{G}$ acts on states by applying move $\sigma \in \mathcal{G}$ to state $x \in \mathcal{G}$ to get state $x^\sigma = x\sigma \in \mathcal{G}$.

Theorem (Jake Vandenberg's conjecture)
There is no Rubik's cube move that cycles through all states.

Recall: states $\leftrightarrow$ moves. Rubik's group $\mathcal{G}$ acts on states by applying move $\sigma \in \mathcal{G}$ to state $x \in \mathcal{G}$ to get state $x^\sigma = x\sigma \in \mathcal{G}$.

Equivalent question: for starting state, WLOG $1 = ()$, is there $\sigma \in \mathcal{G}$ with $\{1^{\sigma^k} : k \in \mathbb{Z}\} = \{1\sigma^k : k \in \mathbb{Z}\} = \{\sigma^k : k \in \mathbb{Z}\} = \mathcal{G}$?

Theorem (Jake Vandenberg's conjecture)
There is no Rubik's cube move that cycles through all states.

Recall: states $\leftrightarrow$ moves. Rubik's group $\mathcal{G}$ acts on states by applying move $\sigma \in \mathcal{G}$ to state $x \in \mathcal{G}$ to get state $x^\sigma = x\sigma \in \mathcal{G}$.

Equivalent question: for starting state, WLOG $1 = ()$, is there $\sigma \in \mathcal{G}$ with $\{1^{\sigma^k} : k \in \mathbb{Z}\} = \{1\sigma^k : k \in \mathbb{Z}\} = \{\sigma^k : k \in \mathbb{Z}\} = \mathcal{G}$? In group theory language:

Theorem (Jake Vandenberg's conjecture)
The Rubik's group $\mathcal{G}$ is not cyclic. (I.e. no $\sigma \in \mathcal{G}$ with $\mathcal{G} = \langle\sigma\rangle$.)

Theorem (Jake Vandenberg's conjecture)
There is no Rubik's cube move that cycles through all states.

Recall: states $\leftrightarrow$ moves. Rubik's group $\mathcal{G}$ acts on states by applying move $\sigma \in \mathcal{G}$ to state $x \in \mathcal{G}$ to get state $x^{\sigma} = x\sigma \in \mathcal{G}$.

Equivalent question: for starting state, WLOG $1 = ()$, is there $\sigma \in \mathcal{G}$ with $\{1^{\sigma^k} : k \in \mathbb{Z}\} = \{1\sigma^k : k \in \mathbb{Z}\} = \{\sigma^k : k \in \mathbb{Z}\} = \mathcal{G}$? In group theory language:

Theorem (Jake Vandenberg's conjecture)
The Rubik's group $\mathcal{G}$ is not cyclic. (I.e. no $\sigma \in \mathcal{G}$ with $\mathcal{G} = \langle \sigma \rangle$.)

Proof.
If $\mathcal{G}$ is cyclic, then $\mathcal{G}$ is abelian.

Theorem (Jake Vandenberg's conjecture)
There is no Rubik's cube move that cycles through all states.

Recall: states $\leftrightarrow$ moves. Rubik's group $\mathcal{G}$ acts on states by applying move $\sigma \in \mathcal{G}$ to state $x \in \mathcal{G}$ to get state $x^\sigma = x\sigma \in \mathcal{G}$.

Equivalent question: for starting state, WLOG $1 = ()$, is there $\sigma \in \mathcal{G}$ with $\{1^{\sigma^k} : k \in \mathbb{Z}\} = \{1\sigma^k : k \in \mathbb{Z}\} = \{\sigma^k : k \in \mathbb{Z}\} = \mathcal{G}$? In group theory language:

Theorem (Jake Vandenberg's conjecture)
The Rubik's group $\mathcal{G}$ is not cyclic. (I.e. no $\sigma \in \mathcal{G}$ with $\mathcal{G} = \langle\sigma\rangle$.)

Proof.
If $\mathcal{G}$ is cyclic, then $\mathcal{G}$ is abelian. But $\mathcal{G}$ is not abelian: $RU \neq UR$. □

Jake’s theorems ii

Theorem (Jake Vandenberg’s theorem)
There is no Rubik’s cube move that when repeated, if starting from the solved state, never returns to the solved state.

Theorem (Jake Vandenberg's theorem)
There is no Rubik's cube move that when repeated, if starting from the solved state, never returns to the solved state.

k-fold repetition of move $\sigma \in G$, applied to solved state $1 = ()$, gives $1^{\sigma^k} = 1\sigma^k = \sigma^k$. Returning to solved state: $\sigma^k = 1$ (for $k \in \mathbb{Z}_+$).

Theorem (Jake Vandenberg's theorem)
There is no Rubik's cube move that when repeated, if starting from the solved state, never returns to the solved state.

k-fold repetition of move $\sigma \in G$, applied to solved state $1 = ()$, gives $1^{\sigma^k} = 1\sigma^k = \sigma^k$. Returning to solved state: $\sigma^k = 1$ (for $k \in \mathbb{Z}_+$).

Equivalent question: does any $\sigma \in G$ have infinite order?

Theorem (Jake Vandenberg's theorem)
There is no Rubik's cube move that when repeated, if starting from the solved state, never returns to the solved state.

k-fold repetition of move $\sigma \in G$, applied to solved state $1 = ()$, gives $1^{\sigma^k} = 1\sigma^k = \sigma^k$. Returning to solved state: $\sigma^k = 1$ (for $k \in \mathbb{Z}_+$).

Equivalent question: does any $\sigma \in G$ have infinite order?

Proposition (corollary of Lagrange's theorem)
If G is finite group and $g \in G$, then order of g divides $|G|$. So $g^{|G|} = 1$.

Theorem (Jake Vandenberg's theorem)
There is no Rubik's cube move that when repeated, if starting from the solved state, never returns to the solved state.

k-fold repetition of move $\sigma \in G$, applied to solved state $1 = ()$, gives $1^{\sigma^k} = 1\sigma^k = \sigma^k$. Returning to solved state: $\sigma^k = 1$ (for $k \in \mathbb{Z}_+$).

Equivalent question: does any $\sigma \in G$ have infinite order?

Proposition (corollary of Lagrange's theorem)
If G is finite group and $g \in G$, then order of g divides $|G|$. So $g^{|G|} = 1$.

Corollary (Jake Vandenberg's theorem)
There is no $\sigma \in \mathcal{G}$ with infinite order (since $\mathcal{G}$ is finite).

Analysing the Rubik’s group

Bases and stabiliser chains i

Definition (Base, stabiliser chain)

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

Bases and stabiliser chains i

Definition (Base, stabiliser chain)

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

Corresponding **stabiliser chain** is

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

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

Definition (Base, stabiliser chain)

If $G \leq \mathrm{Sym}(n)$, distinct elts $B = [\beta_1, \ldots, \beta_r] \subseteq [n]$ 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 $[n]$ such that only $1 \in G$ fixes every $\beta_i \in B$.

(Short base desirable: how to compute minimum base?)

Bases and stabiliser chains i

Definition (Base, stabiliser chain)

If $G \leq \mathrm{Sym}(n)$, distinct elts $B = [\beta_1, \ldots, \beta_r] \subseteq [n]$ 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 $[n]$ such that only $1 \in G$ fixes every $\beta_i \in B$. (Short base desirable: how to compute minimum base?)

Stabiliser chain can be implemented computationally; useful in algorithms (membership testing, random element generation, factorisation into generators).

Example (Rubik's group)

Using GAP:

```
gap> BaseOfGroup( G );
[ 1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21,
    23, 24, 29, 31 ]
gap> Size( last );
18
```

Bases and stabiliser chains ii

Example (Rubik's group)

Using GAP:

```
gap> BaseOfGroup( G );
[ 1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21,
    23, 24, 29, 31 ]
gap> Size( last );
18
```

Base of $\mathcal{G}$ of size 18 is

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

Example (Rubik's group)

Using GAP:

```
gap> BaseOfGroup( G );
[ 1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21,
    23, 24, 29, 31 ]
gap> Size( last );
18
```

Base of $\mathcal{G}$ of size 18 is

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

If move $\sigma \in \mathcal{G}$ fixes every $\beta_i \in B$ then $\sigma = 1$ is empty move.

How many valid states are there? i

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*

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

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

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

Proof.
OST implies $|G^{i-1}| = |\beta_i^{G^{i-1}}||G^{i-1}_{\beta_i}| = |\beta_i^{G^{i-1}}||G^i|$ for each $i = 1, \ldots, r$,

How many valid states are there? i

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*

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

Proof.

OST implies $|G^{i-1}| = |\beta_i^{G^{i-1}}||G^{i-1}_{\beta_i}| = |\beta_i^{G^{i-1}}||G^i|$ for each $i = 1, \ldots, r$, i.e. $|G^{i-1}|/|G^i| = |\beta_i^{G^{i-1}}|$ and $|G^r| = 1$, so

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*

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

Proof.
OST implies $|G^{i-1}| = |\beta_i^{G^{i-1}}||G^{i-1}_{\beta_i}| = |\beta_i^{G^{i-1}}||G^i|$ for each $i = 1, \dots, r$, i.e. $|G^{i-1}|/|G^i| = |\beta_i^{G^{i-1}}|$ and $|G^r| = 1$, so

$$|G| = |G^0| =$$

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*

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

Proof.

OST implies $|G^{i-1}| = |\beta_i^{G^{i-1}}||G^{i-1}_{\beta_i}| = |\beta_i^{G^{i-1}}||G^i|$ for each $i = 1, \ldots, r$, i.e. $|G^{i-1}|/|G^i| = |\beta_i^{G^{i-1}}|$ and $|G^r| = 1$, so

$$|G| = |G^0| = \frac{|G^0|}{|G^1|}\frac{|G^1|}{|G^2|} \cdots \frac{|G^{r-1}|}{|G^r|} =$$

How many valid states are there? i

Theorem (size of perm group)

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

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

Proof.

OST implies $|G^{i-1}| = |\beta_i^{G^{i-1}}||G^{i-1}_{\beta_i}| = |\beta_i^{G^{i-1}}||G^i|$ for each $i = 1, \ldots, r$, i.e. $|G^{i-1}|/|G^i| = |\beta_i^{G^{i-1}}|$ and $|G^r| = 1$, so

$$|G| = |G^0| = \frac{|G^0|}{|G^1|}\frac{|G^1|}{|G^2|}\cdots\frac{|G^{r-1}|}{|G^r|} = |\beta_1^{G^0}||\beta_2^{G^1}|\cdots|\beta_r^{G^{r-1}}|. \qquad \square$$

How many valid states are there? i

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*

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

Example (rotation group of cube)

Compute order of rotation group $G \leq \mathrm{Sym}(8)$ for cube:

How many valid states are there? i

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*

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

Example (rotation group of cube)
Compute order of rotation group $G \leq \mathrm{Sym}(8)$ for cube: base of adjacent vertices say $1, 2$ (once fixed, can't rotate, so $G_{1,2} = 1$).

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

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

Example (rotation group of cube)

Compute order of rotation group $G \leq \mathrm{Sym}(8)$ for cube: base of adjacent vertices say $1, 2$ (once fixed, can't rotate, so $G_{1,2} = 1$).

$|1^G| = 8$ (all vertices);

How many valid states are there? i

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*

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

Example (rotation group of cube)

Compute order of rotation group $G \leq \mathrm{Sym}(8)$ for cube: base of adjacent vertices say $1, 2$ (once fixed, can't rotate, so $G_{1,2} = 1$).

$|1^G| = 8$ (all vertices); in G_1, $|2^{G_1}| = 3$ (vertices adjacent to 1); so

How many valid states are there? i

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

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

Example (rotation group of cube)
Compute order of rotation group $G \leq \mathrm{Sym}(8)$ for cube: base of adjacent vertices say $1, 2$ (once fixed, can't rotate, so $G_{1,2} = 1$).

$|1^G| = 8$ (all vertices); in G_1, $|2^{G_1}| = 3$ (vertices adjacent to 1); so

$$|G| = |1^G||2^{G_1}| = 8 \cdot 3 = 24.$$

How many valid states are there? i

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`).

How many valid states are there? i

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

How many valid states are there? i

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*

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

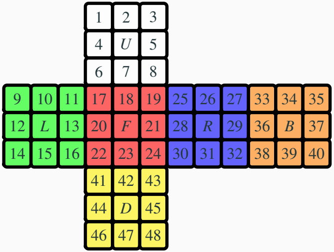
Orbits and stabilisers can be easily computed (e.g. using `GAP`). Implementing base and stabiliser chain for Rubik's group $\mathcal{G}$ (using `BaseOfGroup` and `StabChain` cmds), `GAP` computes:

Corollary
$|\mathcal{G}| = 43\,252\,003\,274\,489\,856\,000 \approx 4.3 \cdot 10^{19}$.
(*Note:* $|\mathcal{G}| = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$. Thus no move of order 13.)

Can this restickering be solved? i

Theorem (Wes's conjecture)

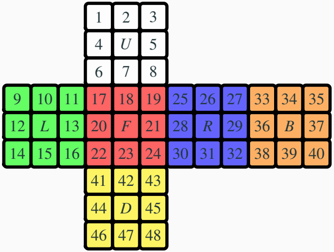
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



Can this restickering be solved? i

Theorem (Wes's conjecture)

"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"

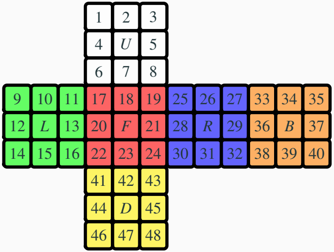


WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

Can this restickering be solved? i

Theorem (Wes's conjecture)

"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



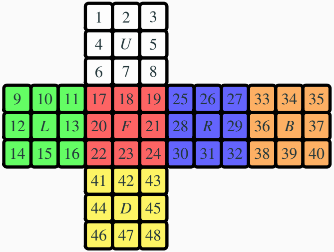
WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28).

Can this restickering be solved? i

Theorem (Wes's conjecture)

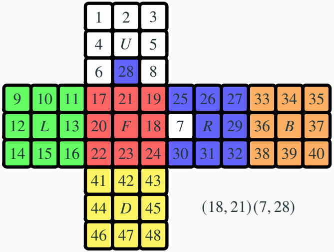
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Theorem (Wes's conjecture)
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



$(18, 21)(7, 28)$

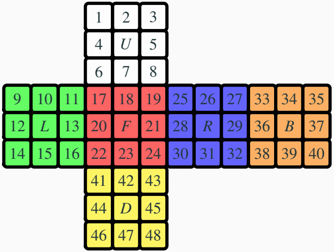
WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Can this restickering be solved? i

Theorem (Wes's conjecture)

"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"

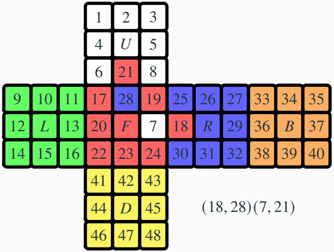


WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Can this restickering be solved? i

Theorem (Wes's conjecture)
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



$(18, 28)(7, 21)$

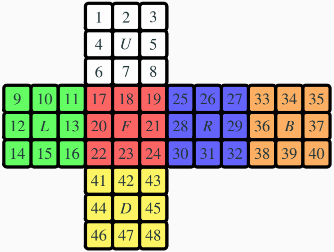
WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Can this restickering be solved? i

Theorem (Wes's conjecture)

"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



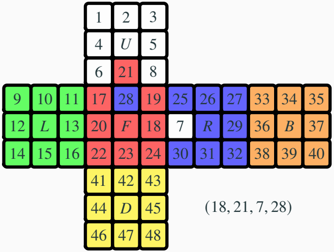
WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Can this restickering be solved? i

Theorem (Wes's conjecture)

"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



$(18, 21, 7, 28)$

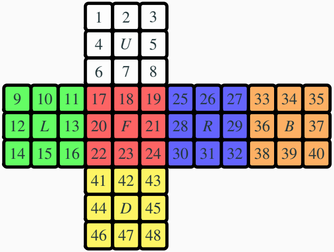
WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Can this restickering be solved? i

Theorem (Wes's conjecture)

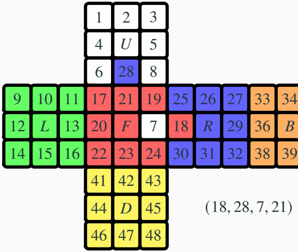
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Theorem (Wes's conjecture)
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

By symmetry, just check one pair, say red/white (18/7) and red/blue (21/28). Four ways: given by where red pieces go (2 options each).

Can this restickering be solved? ii

These restickerings should be invalid states.

Can this restickering be solved? ii

These restickerings should be invalid states. In group theory language:

Theorem (Wes's conjecture)
$(18, 21)(7, 28) \notin \mathcal{G}$, $(18, 28)(7, 21) \notin \mathcal{G}$, $(18, 21, 7, 28) \notin \mathcal{G}$, *and* $(18, 28, 7, 21) \notin \mathcal{G}$.

Can this restickering be solved? ii

These restickerings should be invalid states. In group theory language:

Theorem (Wes's conjecture)
$(18,21)(7,28) \notin \mathcal{G}$, $(18,28)(7,21) \notin \mathcal{G}$, $(18,21,7,28) \notin \mathcal{G}$, *and* $(18,28,7,21) \notin \mathcal{G}$.

Proof.
By GAP:

```
gap> (18,21)(7,28) in G or (18,28)(7,21) in G or
    (18,21,7,28) in G or (18,28,7,21) in G;
false
```

(GAP uses stabiliser chains to verify membership!) □

Can this restickering be solved? ii

These restickerings should be invalid states. In group theory language:

Theorem (Wes's conjecture)
$(18,21)(7,28) \notin \mathcal{G}$, $(18,28)(7,21) \notin \mathcal{G}$, $(18,21,7,28) \notin \mathcal{G}$, *and* $(18,28,7,21) \notin \mathcal{G}$.

Proof.
By GAP:

```
gap> (18,21)(7,28) in G or (18,28)(7,21) in G or
    (18,21,7,28) in G or (18,28,7,21) in G;
false
```

(GAP uses stabiliser chains to verify membership!) □

Can generalise to any two edge pieces (more cases)!

Solving a Rubik's cube... i

We can use `GAP` to solve Rubik's cube state:

Solving a Rubik's cube... i

We can use GAP to solve Rubik's cube state:

```
gap> H := FreeGroup("u","l","f","r","b","d");
<free group on the generators [ u, l, f, r, b, d ]>
gap> h := GroupHomomorphismByImages( H, G, GeneratorsOfGroup( H ),
     GeneratorsOfGroup( G ) );
[ u, l, f, r, b, d ] -> [ (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)
     (11,35,27,19),
  (1,17,41,40)(4,20,44,37)(6,22,46,35)(9,11,16,14)(10,13,15,12),
     (6,25,43,16)(7,28,42,13)(8,30,41,11)(17,19,24,
    22)(18,21,23,20), (3,38,43,19)(5,36,45,21)(8,33,48,24)
     (25,27,32,30)(26,29,31,28),
  (1,14,48,27)(2,12,47,29)(3,9,46,32)(33,35,40,38)(34,37,39,36),
     (14,22,30,38)(15,23,31,39)(16,24,32,40)(41,43,48,
    46)(42,45,47,44) ]
```

($F = \langle u, \ell, f, r, b, d\rangle$ is free group on 6 generators. Then $f : F \longrightarrow \mathcal{G}$ is hom given by $u \mapsto U$, $l \mapsto L$, $f \mapsto F$, $r \mapsto R$, $b \mapsto B$, $d \mapsto D$.)

To simulate scramble, use `GAP` to generate random state $x \in \mathcal{G}$:

Solving a Rubik's cube... ii

To simulate scramble, use `GAP` to generate random state $x \in \mathcal{G}$:

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

$$\begin{aligned} x = {} & (1,27,32,6,43,14,22)(2,28,13,37,18,15,47,42,31) \\ & \quad (3,38,17,24,46,41,9)(5,26)(7,44,39,23,45,34,21,20,12) \\ & \qquad (11,30,40,16,35,33,48)(29,36). \end{aligned}$$

Solving a Rubik's cube... ii

To simulate scramble, use `GAP` to generate random state $x \in \mathcal{G}$:

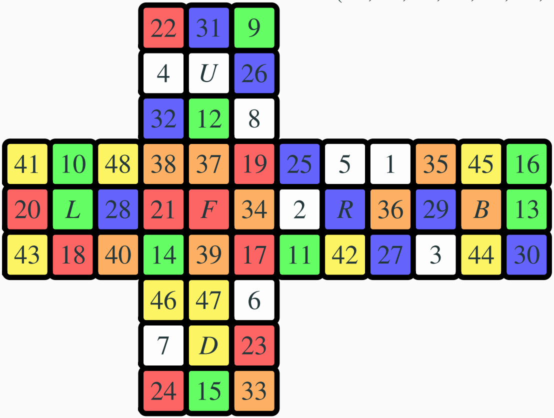
```
gap> x := Random( G );
(1,27,32,6,43,14,22)(2,28,13,37,18,15,47,42,31)(3,38,17,24,46,41,9)
     (5,26)(7,44,39,23,45,34,21,20,12)(11,30,40,16,35,33,48)(29,36)
```

$$x = (1,27,32,6,43,14,22)(2,28,13,37,18,15,47,42,31)$$
$$(3,38,17,24,46,41,9)(5,26)(7,44,39,23,45,34,21,20,12)$$
$$(11,30,40,16,35,33,48)(29,36).$$

Uniform distribution on $\mathcal{G}$ (w.p. $1/|\mathcal{G}| \approx 2.3 \cdot 10^{-20}$).

(*Note:* `GAP` uses stabiliser chain, not sequence of generators.)

$$x = (1,27,32,6,43,14,22)(2,28,13,37,18,15,47,42,31)$$
$$(3,38,17,24,46,41,9)(5,26)(7,44,39,23,45,34,21,20,12)$$
$$(11,30,40,16,35,33,48)(29,36)$$



Solving a Rubik's cube... iv

Factorisation into 78 generators and inverses:

Solving a Rubik's cube... iv

Factorisation into 78 generators and inverses:

```
gap> PreImagesRepresentative( h, x );
l*f^-1*l^-1*f*u*f*u^-1*f^2*l*f*l^-1*u^-1*l^-1*u*l*u^-1*l*u*f*u^-1*f
    ^-1*l^-2*u*l*f^-1*l*f*(l^-1*u)^2*b^-1*u*b*l*u*l^-1*f^-1*l^-1*f*l
    ^2*u*l^-1*u*l*b^-1*u^-1*b*l*d*f^2\
*d^-1*l*f^-1*u*l^-1*f*u^-1*l*d^-1*l*b*d*u^-2*b^-1*r^-1*b*u^-1*r*f^-1*
    u*d^-2
gap> Length( last );
78
```

$$
\begin{aligned}
x = {} & LF^{-1}L^{-1}FUFU^{-1}F^{2}LFL^{-1}U^{-1}L^{-1}ULU^{-1}LUFU^{-1}F^{-1}L^{-2}U \\
& LF^{-1}LF(L^{-1}U)^{2}B^{-1}UBLUL^{-1}F^{-1}L^{-1}FL^{2}UL^{-1}ULB^{-1}U^{-1}BL \\
& DF^{2}D^{-1}LF^{-1}UL^{-1}FU^{-1}LD^{-1}LBDU^{-2}B^{-1}R^{-1}BU^{-1}RF^{-1}UD^{-2}.
\end{aligned}
$$

Solving a Rubik's cube... iv

Factorisation into 78 generators and inverses:

```
gap> PreImagesRepresentative( h, x );
l*f^-1*l^-1*f*u*f*u^-1*f^2*l*f*l^-1*u^-1*l^-1*u*l*u^-1*l*u*f*u^-1*f
    ^-1*l^-2*u*l*f^-1*l*f*(l^-1*u)^2*b^-1*u*b*l*u*l^-1*f^-1*l^-1*f*l
    ^2*u*l^-1*u*l*b^-1*u^-1*b*l*d*f^2\
*d^-1*l*f^-1*u*l^-1*f*u^-1*l*d^-1*l*b*d*u^-2*b^-1*r^-1*b*u^-1*r*f^-1*
    u*d^-2
gap> Length( last );
78
```

$$
\begin{aligned}
x = {} & LF^{-1}L^{-1}FUFU^{-1}F^2LFL^{-1}U^{-1}L^{-1}ULU^{-1}LUFU^{-1}F^{-1}L^{-2}U \\
& LF^{-1}LF(L^{-1}U)^2B^{-1}UBLUL^{-1}F^{-1}L^{-1}FL^2UL^{-1}ULB^{-1}U^{-1}BL \\
& DF^2D^{-1}LF^{-1}UL^{-1}FU^{-1}LD^{-1}LBDU^{-2}B^{-1}R^{-1}BU^{-1}RF^{-1}UD^{-2}.
\end{aligned}
$$

(GAP uses stabiliser chains to factorise almost instantly!)

Solving a Rubik’s cube... v

Check this is correct:

```
gap> x = L*F^(-1)*L^(-1)*F*U*F*U^(-1)*F^2*L*F*L^(-1)*U^(-1)*L^(-1)*U*
     L*U^(-1)*L*U*F*U^(-1)*F^(-1)*L^(-2)*U*L*F^(-1)*L*F*(L^(-1)*U)^2*
     B^(-1)*U*B*L*U*L^(-1)*F^(-1)*L^(-1)*F*L^2*U*L^(-1)*U*L*B^(-1)*U
     ^(-1)*B*L*D*F^2*D^(-1)*L*F^(-1)*U*L^(-1)*F*U^(-1)*L*D^(-1)*L*B*D
     *U^(-2)*B^(-1)*R^(-1)*B*U^(-1)*R*F^(-1)*U*D^(-2);
true
```

Solving a Rubik's cube... v

Check this is correct:

```
gap> x = L*F^(-1)*L^(-1)*F*U*F*U^(-1)*F^2*L*F*L^(-1)*U^(-1)*L^(-1)*U*
     L*U^(-1)*L*U*F*U^(-1)*F^(-1)*L^(-2)*U*L*F^(-1)*L*F*(L^(-1)*U)^2*
     B^(-1)*U*B*L*U*L^(-1)*F^(-1)*L^(-1)*F*L^2*U*L^(-1)*U*L*B^(-1)*U
     ^(-1)*B*L*D*F^2*D^(-1)*L*F^(-1)*U*L^(-1)*F*U^(-1)*L*D^(-1)*L*B*D
     *U^(-2)*B^(-1)*R^(-1)*B*U^(-1)*R*F^(-1)*U*D^(-2);
true
```

To solve state x, apply move $x^{-1} \in \mathcal{G}$ since

Check this is correct:

```
gap> x = L*F^(-1)*L^(-1)*F*U*F*U^(-1)*F^2*L*F*L^(-1)*U^(-1)*L^(-1)*U*
     L*U^(-1)*L*U*F*U^(-1)*F^(-1)*L^(-2)*U*L*F^(-1)*L*F*(L^(-1)*U)^2*
     B^(-1)*U*B*L*U*L^(-1)*F^(-1)*L^(-1)*F*L^2*U*L^(-1)*U*L*B^(-1)*U
     ^(-1)*B*L*D*F^2*D^(-1)*L*F^(-1)*U*L^(-1)*F*U^(-1)*L*D^(-1)*L*B*D
     *U^(-2)*B^(-1)*R^(-1)*B*U^(-1)*R*F^(-1)*U*D^(-2);
true
```

To solve state x, apply move $x^{-1} \in \mathcal{G}$ since $x^{x^{-1}} = xx^{-1} = 1$:

$$
\begin{aligned}
x^{-1} = {} & D^2U^{-1}FR^{-1}UB^{-1}RBU^2D^{-1}B^{-1}L^{-1}DL^{-1}UF^{-1}LU^{-1}FL^{-1}DF^{-2}D^{-1} \\
& L^{-1}B^{-1}UBL^{-1}U^{-1}LU^{-1}L^{-2}F^{-1}LFLU^{-1}L^{-1}B^{-1}U^{-1}B(U^{-1}L)^2F^{-1}L^{-1}F \\
& L^{-1}U^{-1}L^2FUF^{-1}U^{-1}L^{-1}UL^{-1}U^{-1}LULF^{-1}L^{-1}F^{-2}UF^{-1}U^{-1}F^{-1}LFL^{-1}.
\end{aligned}
$$

(Just invert each term in factorisation above and reverse, thus 78 steps.)

Solving a Rubik's cube... v

Check this is correct:

```
gap> x = L*F^(-1)*L^(-1)*F*U*F*U^(-1)*F^2*L*F*L^(-1)*U^(-1)*L^(-1)*U*
     L*U^(-1)*L*U*F*U^(-1)*F^(-1)*L^(-2)*U*L*F^(-1)*L*F*(L^(-1)*U)^2*
     B^(-1)*U*B*L*U*L^(-1)*F^(-1)*L^(-1)*F*L^2*U*L^(-1)*U*L*B^(-1)*U
     ^(-1)*B*L*D*F^2*D^(-1)*L*F^(-1)*U*L^(-1)*F*U^(-1)*L*D^(-1)*L*B*D
     *U^(-2)*B^(-1)*R^(-1)*B*U^(-1)*R*F^(-1)*U*D^(-2);
true
```

To solve state x, apply move $x^{-1} \in \mathcal{G}$ since $x^{x^{-1}} = xx^{-1} = 1$:

$$
\begin{aligned}
x^{-1} = {} & D^2U^{-1}FR^{-1}UB^{-1}RBU^2D^{-1}B^{-1}L^{-1}DL^{-1}UF^{-1}LU^{-1}FL^{-1}DF^{-2}D^{-1} \\
& L^{-1}B^{-1}UBL^{-1}U^{-1}LU^{-1}L^{-2}F^{-1}LFLU^{-1}L^{-1}B^{-1}U^{-1}B(U^{-1}L)^2F^{-1}L^{-1}F \\
& L^{-1}U^{-1}L^2FUF^{-1}U^{-1}L^{-1}UL^{-1}U^{-1}LULF^{-1}L^{-1}F^{-2}UF^{-1}U^{-1}F^{-1}LFL^{-1}.
\end{aligned}
$$

(Just invert each term in factorisation above and reverse, thus 78 steps.)

Not very efficient, since it solves one piece in base B at a time (proceeding up stabiliser chain)... but it works!

Concluding remarks

References i

- Analyzing Rubik's cube with GAP: `https://www.gap-system.org/Doc/Examples/rubik.html`
- J.A. Paulos — Innumeracy (book)