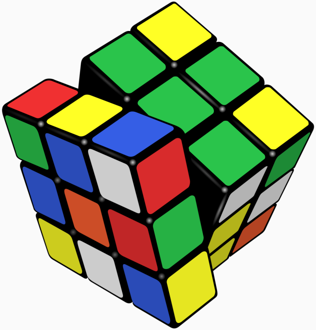
Rubik's cubes and permutation group theory

Lawrence Chen

October 7, 2022

Honours presentation



Contents

Some basic group theory

What is a group? i

Definition (group)

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

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

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

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 $1 = a^0$, 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

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

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.

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 $G = \langle X \rangle$.

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

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

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

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 $a = cb^{-1}$ so $a^k = cb^{-1} \cdots cb^{-1} = c^k b^{-k}$.

Permutations i

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*.

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:

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

σ

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

It means

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:

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

It means

$$1^\sigma = 4,$$

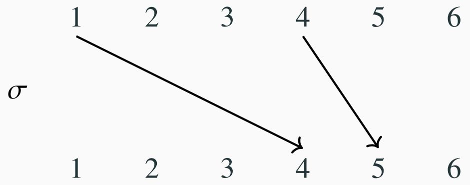
Permutations i

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:



It means

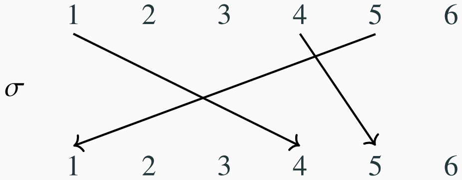
$$1^\sigma = 4,\ 4^\sigma = 5,$$

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

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

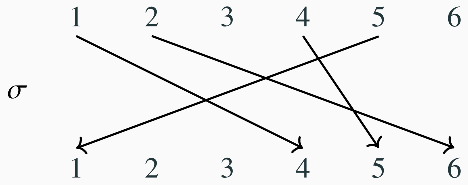
Permutations i

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

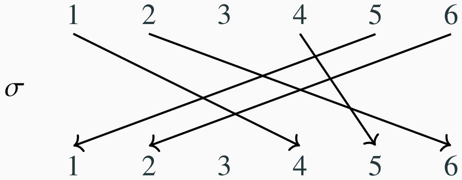
$$1^\sigma = 4,\ 4^\sigma = 5,\ 5^\sigma = 1,\ 2^\sigma = 6,$$

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

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

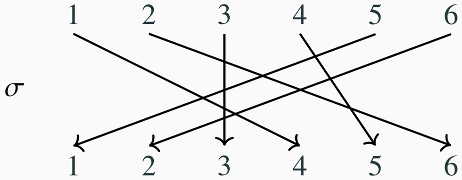
Permutations i

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*.

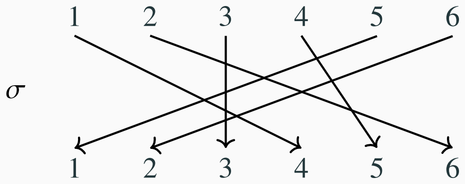
Cycle notation: $\sigma = (1,4,5)(2,6) \in \mathrm{Sym}(6)$ is:



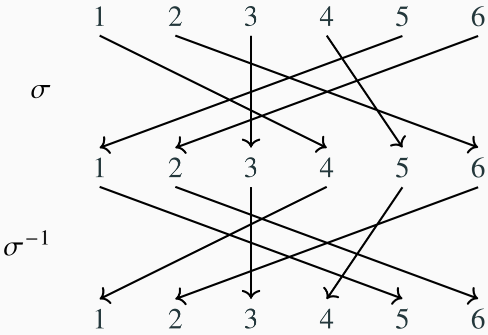
It means

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

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



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



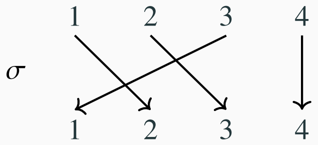
Inverse is $\sigma^{-1} = (1, 5, 4)(2, 6) \in \mathrm{Sym}(6)$.

Permutations iii

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

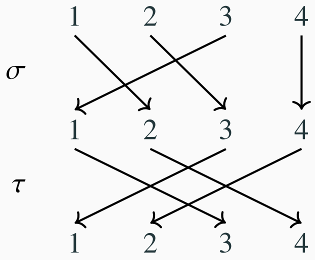
Permutations iii

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



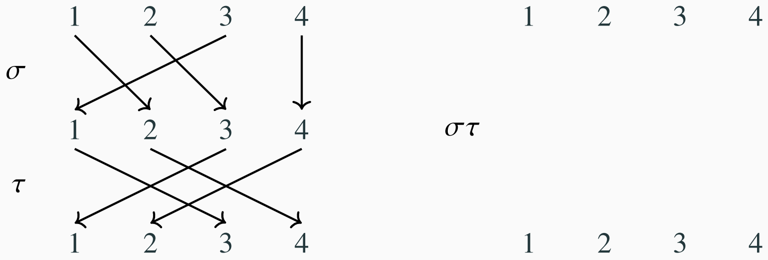
Permutations iii

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

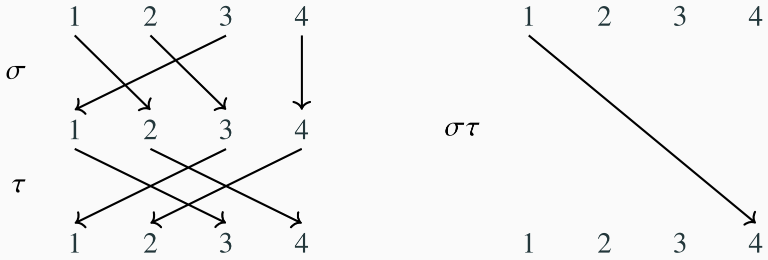
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3), \tau = (1, 3)(2, 4) \in \mathrm{Sym}(4)$,



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

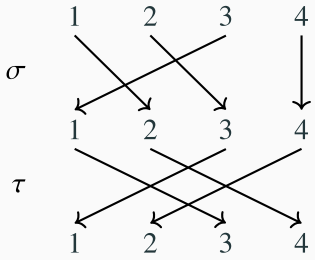
Permutations iii

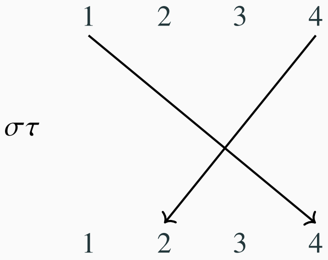
Product/composition: for $\sigma, \tau \in \mathrm{Sym}(n)$, $\sigma\tau$ means "first σ, then τ", so $i^{\sigma\tau} = (i^{\sigma})^{\tau}$. E.g. $\sigma = (1, 2, 3), \tau = (1, 3)(2, 4) \in \mathrm{Sym}(4)$,



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

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

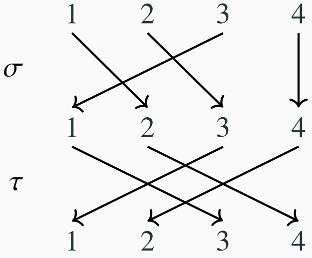


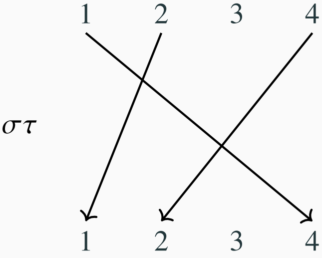


$$\sigma\tau = (1, 2, 3)(1, 3)(2, 4) = (1, 4, 2$$

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

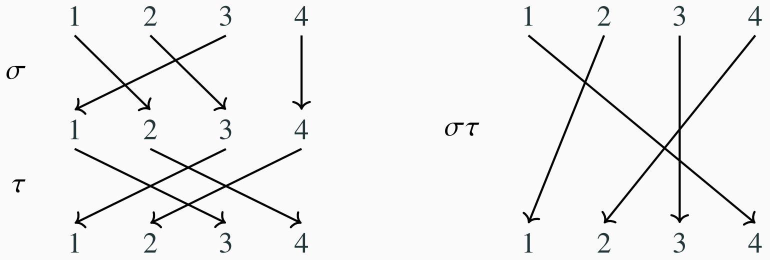




$$\sigma\tau = (1,2,3)(1,3)(2,4) = (1,4,2)$$

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

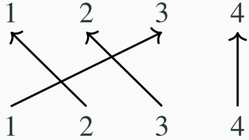
Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

Permutations iv

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

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

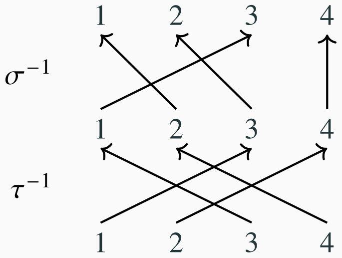
σ^{-1}



Permutations iv

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

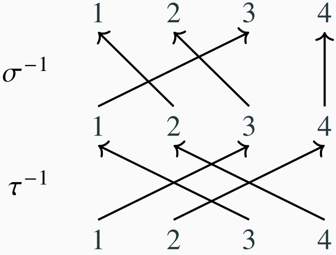
$\sigma^{-1} = (1,3,2)$, $\tau^{-1} = (1,3)(2,4)$,

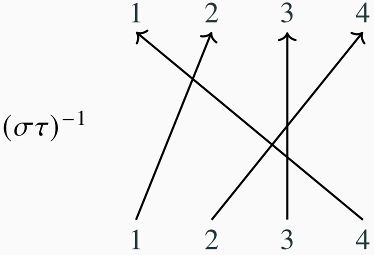


Permutations iv

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

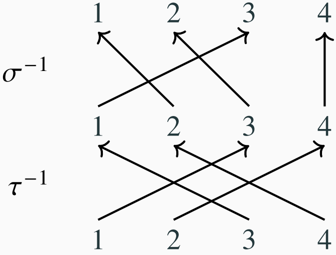
$\sigma^{-1} = (1, 3, 2)$, $\tau^{-1} = (1, 3)(2, 4)$, $(\sigma\tau)^{-1} = (1, 2, 4)$.

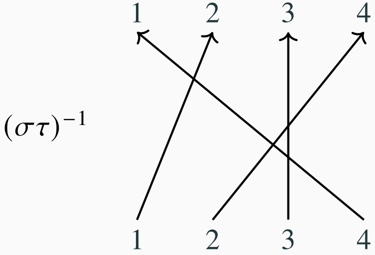




Inverse of product: Is $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$?

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

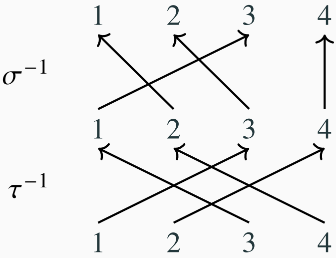


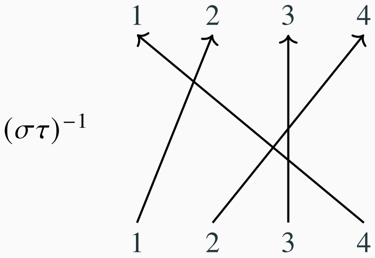


$$\sigma^{-1}\tau^{-1} = (1,3,2)(1,3)(2,4) = (2,3,4) \neq (\sigma\tau)^{-1},$$

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

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.

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.

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 $\Omega \times G \longrightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$ 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 $\alpha \in [n]$, $g \in G$.

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 $\alpha, g \in G$.

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 $g \in G$.

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 $\alpha \in \Omega$.

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).

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

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

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 $\{1\} = 1$ ($\alpha g = \alpha \implies g = 1$).

Group actions iii

Definition (orbit, stabiliser)

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)

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

Definition (orbit, stabiliser)

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

Group actions iii

Definition (orbit, stabiliser)

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)

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)

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)

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)

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

Definition (orbit, stabiliser)

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

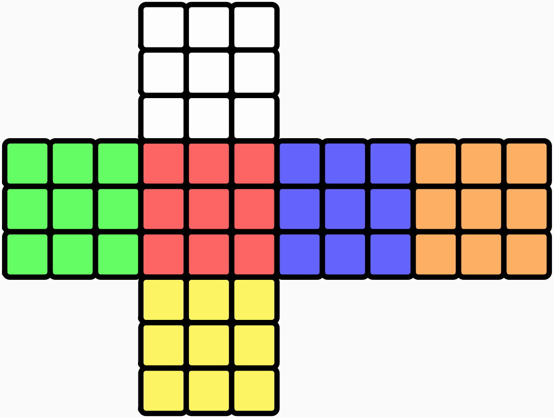
Theorem (orbit-stabiliser)

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

The Rubik's group

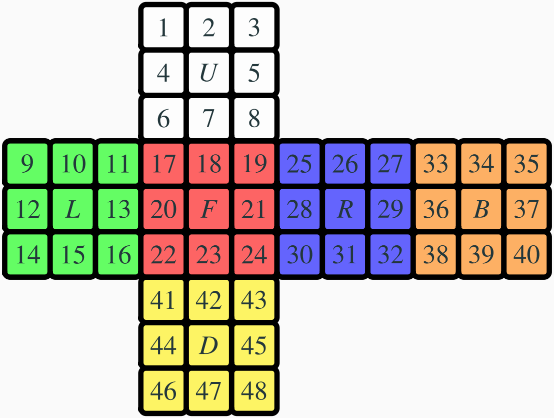
Representing the cube and its moves i

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



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

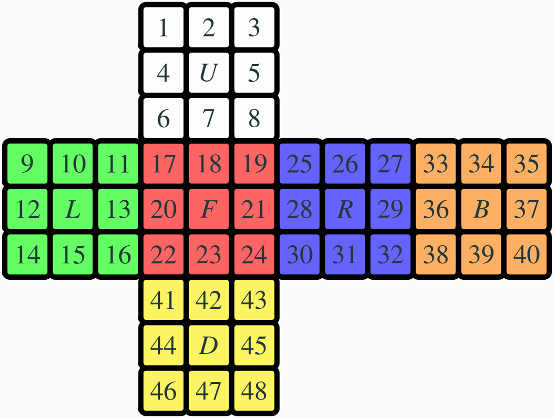
In **solved state**, label smaller faces (except each centre) using $[48]$:



Representing the cube and its moves i

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

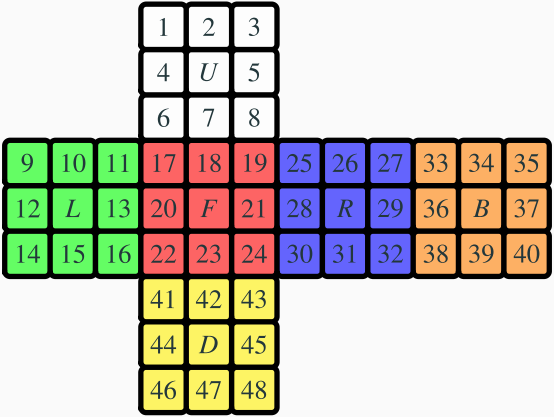
In **solved state**, label smaller faces (except each centre) using $[48]$:



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

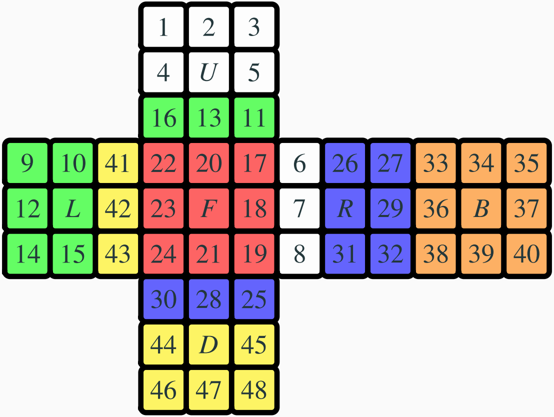
Representing the cube and its moves ii

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



Representing the cube and its moves ii

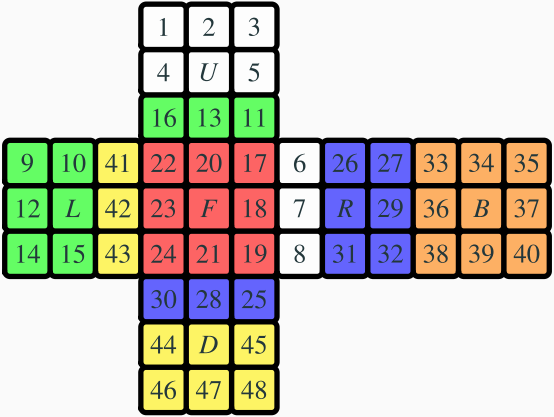
From *solved state*, consider F which rotates front face clockwise:



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*, 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 elementary moves 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 elementary moves 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 elementary moves 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 elementary moves 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: inverse elementary moves 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: inverse elementary moves 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: inverse elementary moves 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: inverse elementary moves 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: inverse elementary moves 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

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

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

Representing the cube and its moves iv

In cubing community: inverse elementary moves 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: inverse elementary moves 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: inverse elementary moves 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: inverse elementary moves 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 $i \in [n]$.

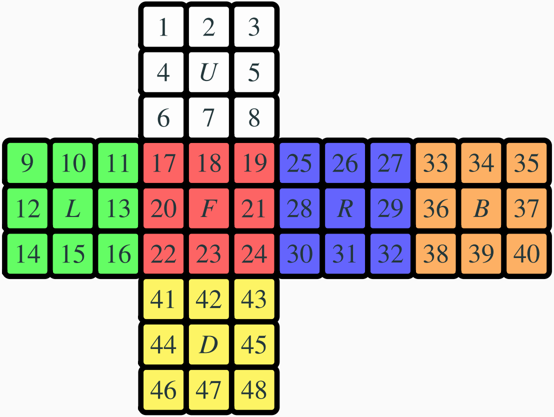
Moves *don't generally commute*: $RU \neq UR$ since

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

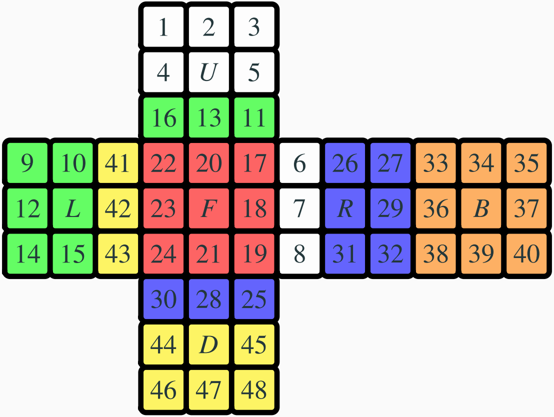
$$19^{RU} = (19^R)^U = 3^U = 8 \quad \text{but} \quad 19^{UR} = (19^U)^R = 11^R = 11.$$

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

Let $\mathcal{G}$ be valid **moves**; can represent move $\sigma \in \mathcal{G}$ as 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**; can represent state $x \in \mathcal{S}$ as element of Sym(48) giving permutation of labels to solved state $1 = ()$. (I.e. i^x is label at x-position of i in solved state 1.)

Let $\mathcal{G}$ be valid **moves**; can represent move $\sigma \in \mathcal{G}$ as 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**; can represent state $x \in \mathcal{S}$ as element of Sym(48) giving permutation of labels to solved state $1 = ()$. (I.e. i^x is label at x-position of i in solved state 1.)

Let $\mathcal{G}$ be valid **moves**; can represent move $\sigma \in \mathcal{G}$ as 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 $1 = ()$.

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**; can represent state $x \in \mathcal{S}$ as element of $\mathrm{Sym}(48)$ giving permutation of labels to solved state $1 = ()$. (I.e. i^x is label at x-position of i in solved state 1.)

Let $\mathcal{G}$ be valid **moves**; can represent move $\sigma \in \mathcal{G}$ as 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 $1 = ()$.

So moves $\leftrightarrow$ states for Rubik's cube; as sets, $\mathcal{S} = \mathcal{G}$.

The Rubik's group of permutations i

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

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 elementary moves/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 elementary moves/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 elementary moves/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:* $G = \langle U, L, F, R, B, D \rangle$.

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 elementary moves/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 elementary moves/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 );
```

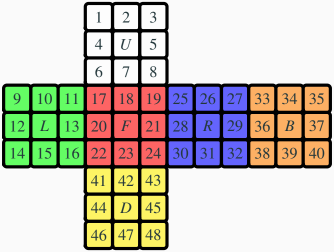
The Rubik's group of permutations ii

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?*

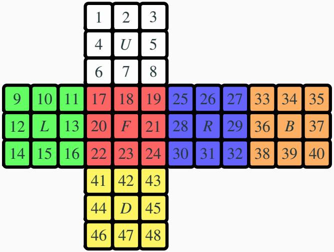
Orbits and stabilisers i




```
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 ]
```

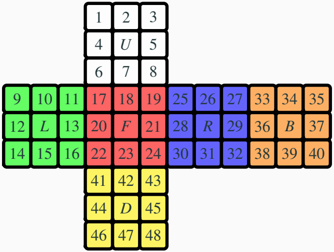
Two $\mathcal{G}$-orbits: corner pieces $1^{\mathcal{G}}$, edge pieces $2^{\mathcal{G}}$.

Orbits and stabilisers ii



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 ii



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 $\operatorname{lcm}(4, 4, 4, 4, 4) = 4$.
- *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 $\operatorname{lcm}(6, 3, 6, 3) = 6$.

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 $\operatorname{lcm}(3, 3, 3, 3, 3) = 3$.

- *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 $\mathrm{lcm}(3, 3, 3, 3, 3) = 3$.
- *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

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

Element 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

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

Jake's theorems i

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 $x^\sigma = x\sigma \in \mathcal{G}$.

Jake's theorems i

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 $\{1^{\sigma^k} : k \in \mathbb{Z}\} = \{1\sigma^k : k \in \mathbb{Z}\} = \{\sigma^k : k \in \mathbb{Z}\} = \mathcal{G}$?

Jake's theorems i

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 $\mathcal{G} = \langle \sigma \rangle$.)

Jake's theorems i

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: $RU \neq UR$. $\square$

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 $g^{|G|} = 1$.

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 $g^{|G|} = 1$.

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

TODO

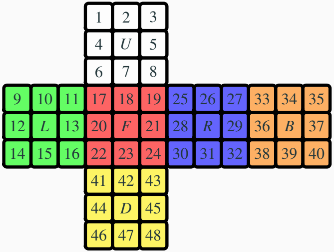
How many valid states are there? i

TODO

Can this restickering be solved? i

Theorem (Wes's conjecture)

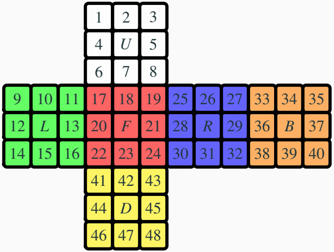
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



Can this restickering be solved? i

Theorem (Wes's conjecture)

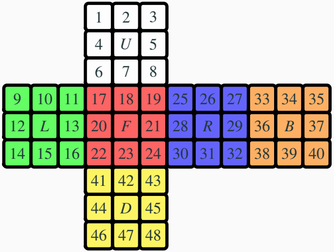
"I'm 99% sure you can't swap two [adjacent] edge pieces without affecting another piece?!"



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?!"

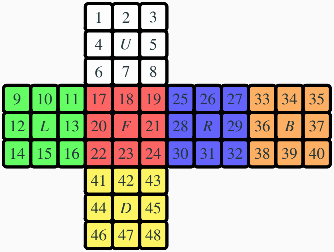


WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

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?!"

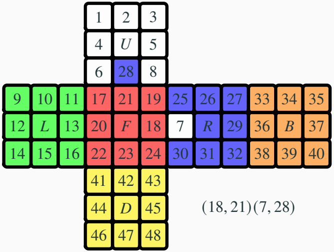


WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

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?!"



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

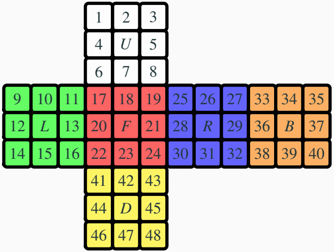
WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

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?!"



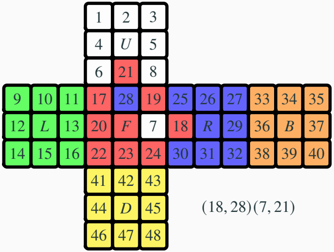
WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

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?!"



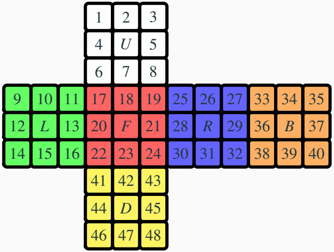
$(18, 28)(7, 21)$

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?!"

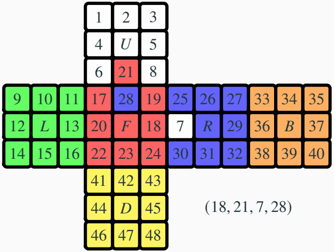


WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

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?!"



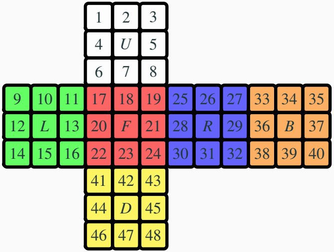
$(18, 21, 7, 28)$

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?!"

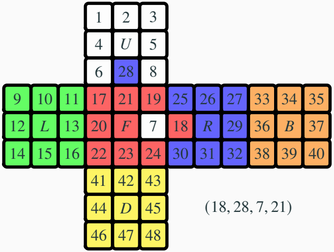


WLOG consider solved state. *Equivalent question:* does only restickering two adjacent edge pieces give solvable state?

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).

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? 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 bases and stabiliser chains to verify membership!) □

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

Solving a Rubik's cube... i

TODO

Concluding remarks

References i

- Analyzing Rubik's cube with GAP: `https://www.gap-system.org/Doc/Examples/rubik.html`