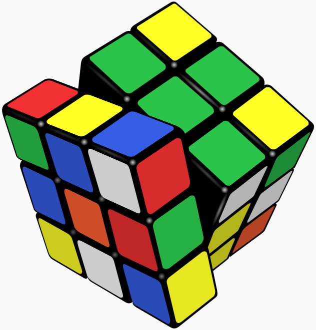
Rubik's cubes and permutation group theory

Lawrence Chen

October 7, 2022

Honours presentation



Contents

Some basic group theory

The Rubik’s group

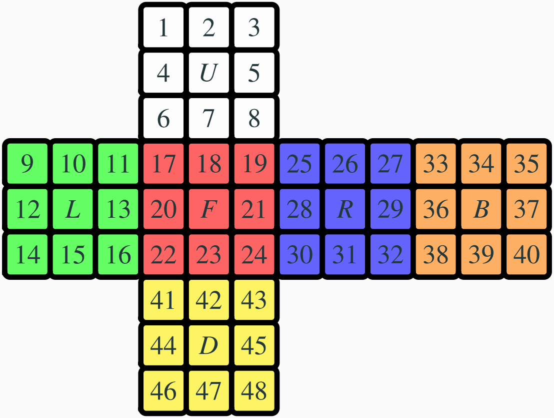
Representing the cube and its moves i

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).

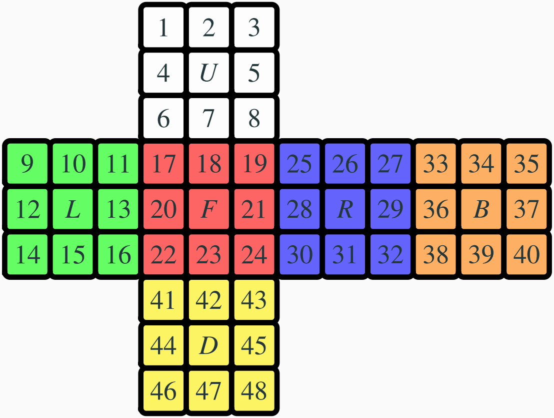
In **solved state**, label smaller faces (except each centre) using $[48]$:



Representing the cube and its moves i

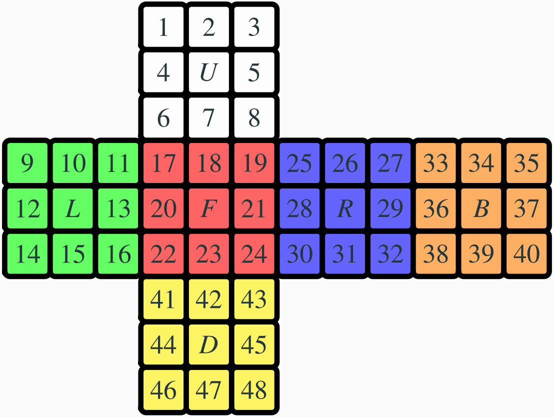
A Rubik's cube has 6 large faces (each with 3×3 smaller faces).

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



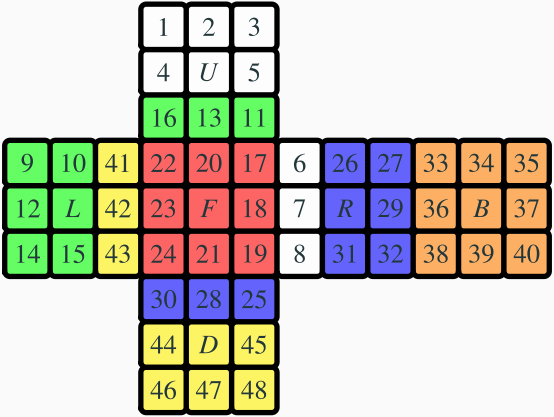
6 **elementary moves (generators)**: U, L, F, R, B, D (rot. *clockwise*).

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



Representing the cube and its moves ii

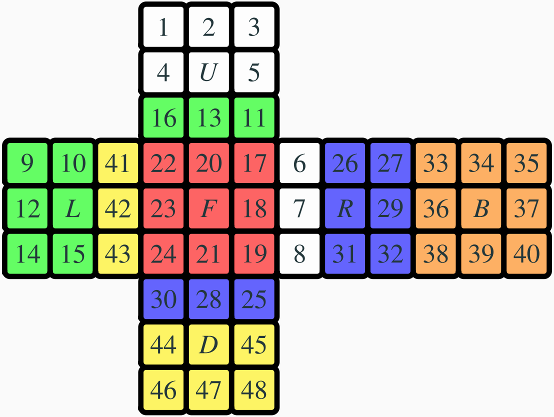
From *solved state*, consider F which rotates front face clockwise:



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. $RUR^{-1}U^{-1}$, $URU^{-1}L^{-1}UR^{-1}U^{-1}L$, 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: $1 = RR^{-1}$).

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

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

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

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

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

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

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

Recall: $\sigma = \tau$ in $\mathrm{Sym}(n)$ iff $i^\sigma = i^\tau$ for all $i \in [n]$.

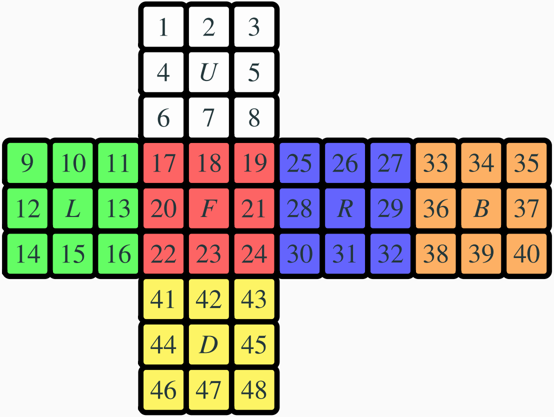
Moves *don't generally commute*: $RU \neq UR$ since

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

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

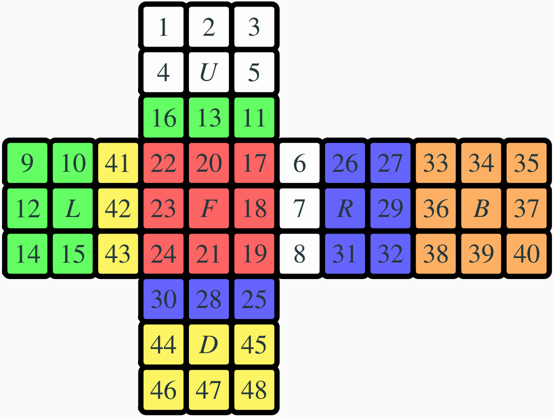
Moves vs states for Rubik's cube i

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



Moves vs states for Rubik's cube i

(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

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

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

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

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 $1 = ()$.

Moves vs states for Rubik's cube ii

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 $1 = ()$.

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.

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.

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

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.

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 );
```

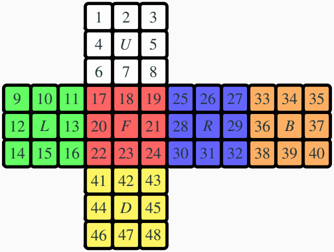
The Rubik’s group of permutations ii

`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 );
```

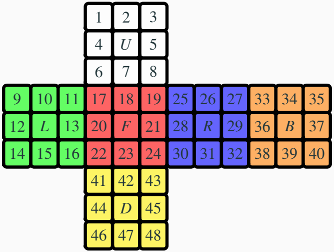
`Order` cmd: $|\mathcal{G}| = 43\,252\,003\,274\,489\,856\,000 \approx 4.3 \cdot 10^{19}$. *How?*

Orbits and stabilisers i



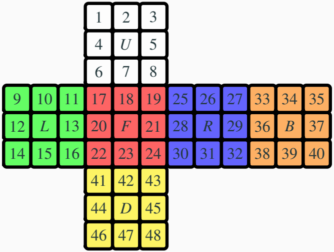

```
gap> Orbit( G, 1 );
[ 1, 6, 40, 27, 8, 35, 16, 41, 32, 25, 48, 3, 11, 24, 46, 33, 43, 17,
      30, 14, 19, 9, 22, 38 ]
gap> Orbit( G, 2 );
[ 2, 5, 12, 7, 36, 10, 47, 4, 28, 45, 34, 13, 29, 44, 20, 42, 26, 21,
      37, 15, 31, 18, 23, 39 ]
```

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



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

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

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 $\text{lcm}(15,7,3,7) = 105$.

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

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 ↔ 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 $k \in \mathbb{Z}_+$).

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.

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

Concluding remarks

References i

- TODO