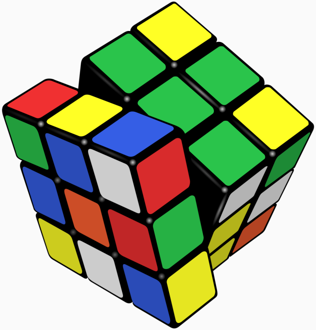
Minimum bases in permutation groups

Lawrence Chen

October 25, 2022

Honours presentation
Monash University
Supervised by A/Prof. Heiko Dietrich and
Dr Santiago Barrera Acevedo



Contents

Aim: analyse Blaha's 1992 paper on NP-completeness of min base problem, and recent results for primitive perm groups.

Motivation: understanding the Rubik's cube

- How can we represent *operations* of a cube?
- *How many* states does a Rubik's cube have?
- How can we better *understand* operations of a cube?

One answer: using permutations and *computational group theory*!

(J. A. Paulos, Innumeracy)

> *Ideal Toy Company stated on the package of the original Rubik cube that there were* ***more than three billion*** *possible states the cube could attain. It's analogous to McDonald's proudly announcing that they've sold* ***more than 120*** *hamburgers.*

Some basic group theory

Permutations

Definition (permutation)

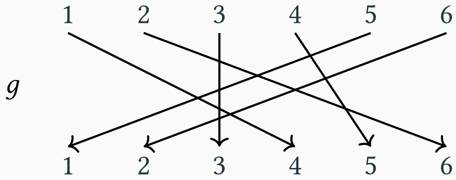
Permutation of Ω is bijection $g : \Omega \to \Omega$.

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

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

Write $1 = ()$ for identity. Write i^g instead of $g(i)$ for *image*.

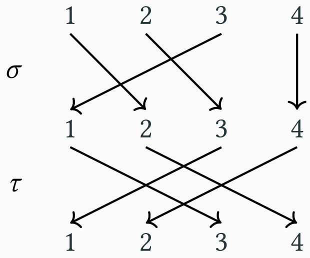
Cycle notation: $g = (1, 4, 5)(2, 6) \in \mathrm{Sym}(6)$ is:

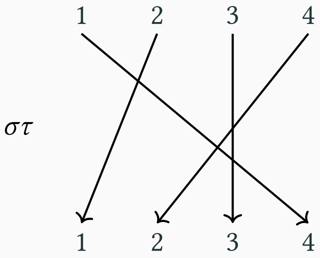


It means $1^g = 4,\ 4^g = 5,\ 5^g = 1,\ 2^g = 6,\ 6^g = 2,\ 3^g = 3.$

Permutations (ii)

Product/composition: for $g, h \in \mathrm{Sym}(\Omega)$, gh means “first g, then h”, so $\alpha^{gh} = (\alpha^g)^h$. E.g. $g = (1,2,3) \in \mathrm{Sym}(4)$, $h = (1,3)(2,4) \in \mathrm{Sym}(4)$,





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

Note: here, $gh \neq hg$, since $1^{gh} = 4$ but $1^{hg} = (1^h)^g = 3^g = 1$. Identity $1 = ()$ satisfies $1g = g1 = g$ for $g \in \mathrm{Sym}(\Omega)$.

Definition (permutation group)

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

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

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

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

Definition (generator)

Set X **generates** G if every $g \in G$ is $g = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ for some $r \in \mathbb{N}$, $x_i \in X$ **generators**, $\varepsilon_i \in \{\pm 1\}$; write $G = \langle X \rangle$.

Example (dihedral group)

Let $r = (1, 2, 3, 4)$, $s = (1, 4)(2, 3) \in \mathrm{Sym}(4)$. **Dihedral group** of order 8 is $D_8 := \langle r, s \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ (e.g. $srs^{-1}r^2 = r$), *"symmetries of square"* .

Definition (group action)

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

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

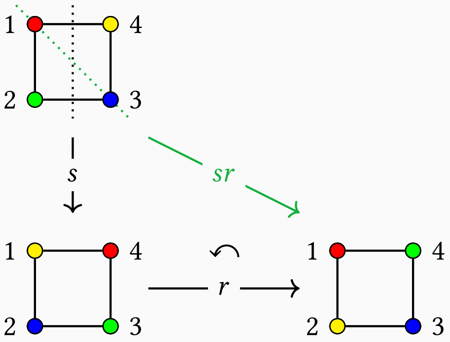
Example (natural action)

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

Example (dihedral group)

Recall $D_8 = \langle r, s \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ acts naturally on $[4]$.

Note: $r = (1,2,3,4)$, $s = (1,4)(2,3)$, $sr = (2,4)$. Visualise D_8-action by labelling vertices of square by $[4]$: $g \in D_8$ sends vertex at i to i^g.



Orbits and stabilisers

Definition (orbit)

If G acts on $\mathcal{S}$, then **orbit** of $\alpha \in \mathcal{S}$ is $\alpha^G := \{\alpha^g : g \in G\}$.

Idea: states $\alpha^g \in \mathcal{S}$ reachable from fixed $\alpha \in \mathcal{S}$ by moves $g \in G$.

One orbit only: **transitive** action.

Definition (stabiliser)

If G acts on $\mathcal{S}$, then **stabiliser** of $\alpha \in \mathcal{S}$ is $G_\alpha := \{g \in G : \alpha^g = \alpha\}$.

Idea: moves $g \in G$ that fix given $\alpha \in \mathcal{S}$.

Orbits and stabilisers (ii)

Orbit α^G: states $\alpha^g \in \mathcal{S}$ reachable from fixed α by moves $g \in G$.

Stabiliser G_α: moves $g \in G$ that fix given α.

Example (dihedral group)

Recall $G = D_8 = \langle r, s\rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \leq \mathrm{Sym}(4)$ where $r = (1, 2, 3, 4)$, $s = (1, 4)(2, 3)$.

Orbit of 1: $1^1 = 1$, $1^r = 2$, $1^{r^2} = 3$, $1^{r^3} = 4$, so $1^G = [4]$ (*transitive*).

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

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

Theorem (orbit-stabiliser)

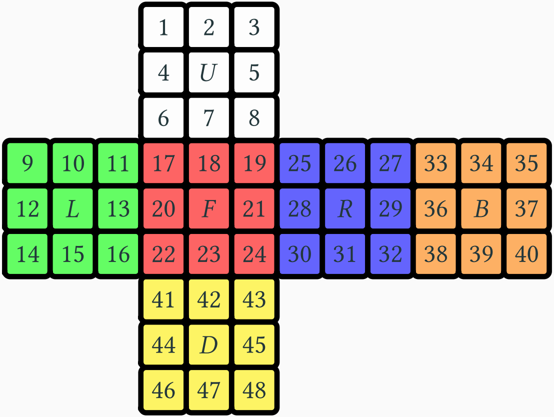
If G acts on $\mathcal{S}$, then for $\alpha \in \mathcal{S}$, $|\alpha^G||G_\alpha| = |G|$.

The Rubik's group

Representing the cube and its operations

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

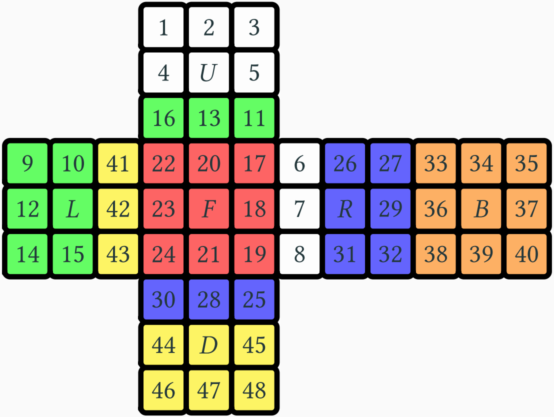
In **solved state** 1, label stickers (except each centre) using $[48]$:



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

Representing the cube and its operations (ii)

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



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

The Rubik's group of permutations

Generators as permutations of labels $[48]$:

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

Operation is sequence of generators and inverses. E.g. $RUR^{-1}U^{-1}$, $URU^{-1}L^{-1}UR^{-1}U^{-1}L$, $RUR^{-1}URU^2R^{-1}U^2$, $1 = ()$.

Definition (Rubik's group)

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

Clearly $\mathcal{G}$ is finite, but what is $|\mathcal{G}|$?

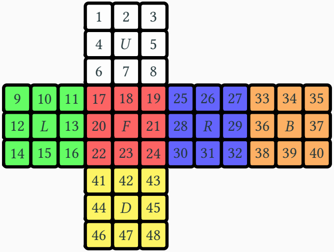
The Rubik's group of permutations (ii)

GAP code to define generators and $\mathcal{G} = \langle U, L, F, R, B, D \rangle$ (as G):

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

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

Orbits in the Rubik's group




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

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

Transitive action on corners

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

Examples of blocks: singletons, $\mathcal{S}$, orbits.
Block is **nontrivial** if $|\Delta| > 1$ and $\Delta \neq \mathcal{S}$.

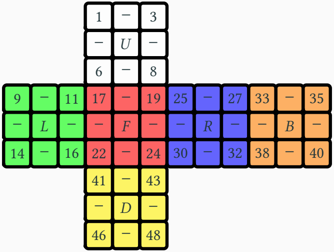
Definition (primitivity)
A *transitive* G-action is **primitive** if there are no nontrivial blocks; otherwise it is **imprimitive**.

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

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

Transitive action on corners (ii)

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

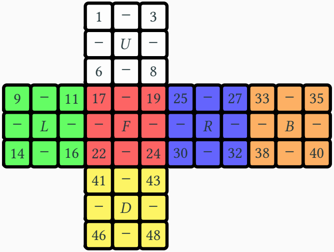


$$\Sigma = \{\overbrace{\{1, 35, 9\}}^{UBL}, \overbrace{\{6, 11, 17\}}^{ULF}, \overbrace{\{40, 46, 14\}}^{BDL}, \overbrace{\{27, 3, 33\}}^{RUB},$$

$$\underbrace{\{8, 25, 19\}}_{URF}, \underbrace{\{16, 41, 22\}}_{LDF}, \underbrace{\{32, 48, 38\}}_{RDB}, \underbrace{\{24, 43, 30\}}_{FDR}\}$$

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

Transitive action on corners (iii)



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

$$F \mapsto (\underbrace{\{6, 11, 17\}}_{ULF}, \underbrace{\{8, 25, 19\}}_{URF}, \underbrace{\{24, 43, 30\}}_{FDR}, \underbrace{\{16, 41, 22\}}_{LDF}) \in \mathrm{Sym}(\Sigma).$$

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

Bases and stabiliser chains

Bases and stabiliser chains

Definition (Base, stabiliser chain)

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

Corresponding **stabiliser chain** is

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

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

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

Theorem (Blaha, 1992)

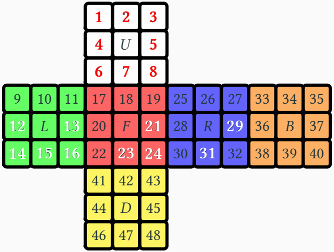
Problem of finding minimum base for G is NP-complete (if $\mathrm{P} \neq \mathrm{NP}$, then no polynomial time algorithm).

Example (Rubik's group)

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

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

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



Bases and stabiliser chains (iii)

Stabiliser chain implemented in GAP; useful in algorithms.

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

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

Problem (random element generation)

Generate uniformly random element of G.

(*Alternative:* random product of generators in X — Markov chain; mixing time/distribution?)

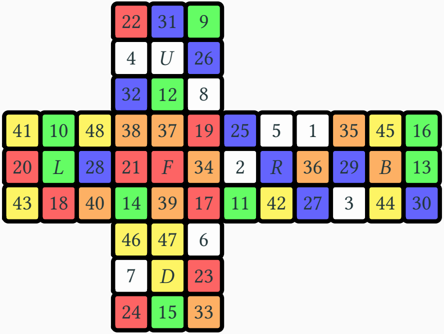
Bases and stabiliser chains (iv)

Stabiliser chain implemented in GAP; useful in algorithms.

Problem (membership testing)

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

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



What is the size of the Rubik's group?

Theorem (size of perm group)

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

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

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

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

Corollary

For Rubik's group $\mathcal{G}$, $|\mathcal{G}| = 43\,252\,003\,274\,489\,856\,000 \approx 4.3 \cdot 10^{19}$.

Base sizes of primitive groups

Definition

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

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

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

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

Definition

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

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

Non-large base permutation groups

Theorem (Liebeck, 1984)

For primitive perm group G of degree n, either:

(i) *G is "large base"; or*

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

Previous best (Babai, 1981): $b(G) = O(\sqrt{n})$ if not containing $\mathrm{Alt}(n)$.

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

Non-large base permutation groups (ii)

Theorem (Moscatiello & Roney-Dougal, 2021)

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

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

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

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

Question (Moscatiello & Roney-Dougal, 2021)

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

Main result in thesis

Theorem

Let $G \leq \mathrm{AGL}_d(2)$ *be primitive for some* $d \leq 10$ *with natural action on* K^d *with* $b(G) = d + 1$*. (Then* G *is perm group of degree* $n = 2^d$*.) Then:*

(i) G *is* $\mathrm{AGL}_d(2)$ *with* $d \geq 2$*; or*

(ii) G *is* $\mathrm{Sp}_d(2) \ltimes C_2^d$ *with* $d \geq 4$ *even.*

Main result in thesis (ii)

Proof (idea).

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

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

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

Main result in thesis (iii)

From above theorem, we conjecture the following:

Conjecture

Primitive group $G \leq \mathrm{Sym}(n)$ satisfies $b(G) = \log n + 1$ iff $n = 2^d$ and:

- G is $\mathrm{AGL}_d(2)$ with $d \geq 2$; or
- G is $\mathrm{Sp}_d(2) \ltimes C_2^d$ with $d \geq 4$ even.

Concluding remarks

Acknowledgements

I would like to express my gratitude to my supervisors Heiko and Santiago. I appreciate their tireless effort in imparting their knowledge. To all the course lecturers and instructors I've had this year, who I have learned much from.

I would also like to thank my friends in the Honours cohort, especially Jeremy, Will, and Clayton, for their friendship and support over the year. For Puti too, who has helped me so much.

I would like to thank my parents, for doing so much for me. Also, Wes for being my greatest support, and sparking my interest in Rubik's cubes. To Chris, whose godly wisdom has sharpened me in so many ways. Also, to all my church group members and fellow leaders, for their constant support and care.

Lastly, I would like to thank God for His guiding hand in my life. In the midst of busyness and challenges this year, His presence has given me hope, rest and security. I thank Him for this Honours experience in this season of my life.

"There is a time for everything,
and a season for every activity under the heavens"

— Ecclesiastes 3:1 (NIV)

References and resources

- Analyzing Rubik's cube with GAP:
  https://www.gap-system.org/Doc/Examples/rubik.html
- J. A. Paulos — *Innumeracy* (book)
- Holt — *Handbook of Computational Group Theory* (textbook)
- Dixon and Mortimer — *Permutation Groups* (textbook)
- Blaha — *Minimum bases for permutation groups: The greedy approximation*, 1992:
  https://doi:10.1016/0196-6774(92)90020-D
- Liebeck — *On minimal degrees and base sizes of primitive permutation groups*, 1984: https://doi.org/10.1007/bf01193603
- Moscatiello and Roney-Dougal: *Base sizes of primitive permutation groups*, 2021: https://doi.org/10.1007/s00605-021-01599-5

References and resources (ii)

The **order** of $g \in G \leq \mathrm{Sym}(\Omega)$ is smallest $k \in \mathbb{Z}_+$ such that $g^k = 1$.
Fact: order of g is lcm of cycle lengths; it divides $|G|$.

Note: for Rubik's group, R has order 4, $RUR^{-1}U^{-1}$ has order 6, RU has order 105 (GAP). Order 7? $(RU)^{15}$. Order 13? None;

$$|\mathcal{G}| = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11.$$

- *Bonus:* Orders of elements in Rubik's group (1260 largest, 13 smallest without, 11 rarest, 60 most common, median 67.3, 73 options): `https://www.jaapsch.net/puzzles/cubic3.htm#p34`
- *Bonus:* Thistlethwaite's 52 move algorithm (using group theory): `https://www.jaapsch.net/puzzles/thistle.htm`

Large base definition

Definition

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

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

for some m, r, k, where $\mathrm{Sym}(m)$ acts on $\binom{[m]}{k}$, and if $r > 1$ then wreath product has *product action* of degree $n = \binom{m}{k}^r$.