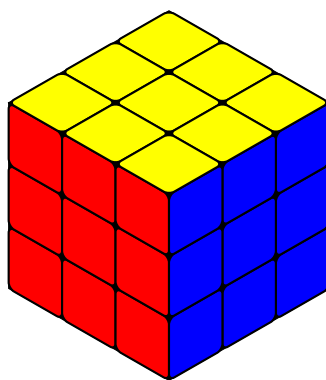


On the order of 3×3 Rubik's cube permutations

Julia PHAM BA NIEN

January 25, 2024



Contents

1	Introduction to group theory	3
1.1	Groups	3
1.2	Permutations	4
2	Topology of a rubik's cube	8
2.1	Pieces of the cube	8
2.2	State as a permutation	10
2.3	Moves, algorithms and notations	11
2.3.1	Rotations	11
2.3.2	Turns	11
2.4	Centers	13
2.5	Edges	13
2.6	Corners	15
2.7	Valid state	16
2.8	Order of rubik's cube permutations	17

This article is a plan to give some good intuition over the rubik's cube and group theory to some classmates (♥), thus I'll take more time to prove things which may not be "necessary", all for giving intuition.

I try to make it accessible to highschoolers (which isn't the level of my classmates), thus why I introduce concepts which are "common", but that won't stop me from expressing ideas that are "advanced", I'll just introduce them (if they are short enough, I won't speak about resoluble groups, galois groups, Jordan-Hölder decomposition, etc. despite them being quite interesting, but what I meant is that there are stuffs to learn even if you aren't an highschooler).

1 Introduction to group theory

1.1 Groups

Definition 1 (Group). *Let G be a non-empty set, and $\cdot : G \times G \rightarrow G$ an application, we say that (G, \cdot) forms a group if:*

- (associativity) $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$, so for ease of notation, no superfluous parenthesis will be used.
- (unity) $\exists ! e \in G, \forall x \in G, x \cdot e = x = e \cdot x$, I'll always refer to that element, called the neutral element, when writing e .
- (inverse) $\forall x \in G, \exists ! y \in G, x \cdot y = e = y \cdot x$, I'll always write this y as x^{-1} .

Convention 1. *When which \cdot we use is obvious, we'll say that G is a group.*

Convention 2. *When which \cdot we use is obvious, we'll write xy instead of $x \cdot y$.*

Definition 2 (Subgroup). *We have (H, \cdot) subgroup of (G, \cdot) if $(H, \cdot), (G, \cdot)$ are both groups and $H \subseteq G$.*

We'll suppose in this section that G is a group.

Definition 3 (Conjugation). *Let $a, b \in G$, we say that $a^{-1}ba$ is the conjugation of b by a and we write this element b_a .*

Definition 4 (Commutator). *Let $a, b \in G$, we say that $a^{-1}b^{-1}ab$ is the commutator of b by a and we write this element $[a, b]$.*

Convention 3. *I'll denote by \mathbb{N} the set of natural number following the French convention/peano's construction, which is: $\{n \in \mathbb{Z} | n \geq 0\}$.*

Definition 5 (Generator). *We have G a group generated by elements $x_1, \dots, x_n \in G$ (the generator) if*

$$\forall x \in G, \exists n \in \mathbb{N}, \exists (w_i \in \{x_1, \dots, x_n\})_{i \in \llbracket 1, n \rrbracket}, x = \prod_{i=1}^n w_i$$

Notation 1 (Generator). *If G is generated with (x_1, \dots, x_n) , then we can write*

$$G = \langle x_1, \dots, x_n \rangle$$

1.2 Permutations

Until the end of this section, n will be a natural number.

Definition 6 (Permutation). *A permutation is an element of S_n , where S_n is the group of bijection of $\llbracket 1, n \rrbracket$ with application composition or any group isomorphic to a subgroup of S_n .*

For ease of introduction I'll mostly talk about S_n but this theory will be useful for thinking about rubik's cubes, which as you may guess isn't of the form $\llbracket 1, n \rrbracket$ but is isomorphic to a subgroup of thereof.

A "good" way to think about permutation is to think of them as shufflers or elements.

Notation 2 (Permutation). *Let $\sigma \in S_n$, we can refer to σ with the notation*

$$\sigma =: \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

And we can remove the column i of this notation where the element on top and on the bottom are the same or swap the order of the columns.

If there are no column where the top and the bottom are equal, we say that the notation is reduced.

Definition 7 (Support). *Let $\sigma \in S_n$, the support is $\text{supp}(\sigma) := \{\sigma(i) \neq i \mid i \in \llbracket 1, n \rrbracket\}$.*

Theorem 1 (commutativity of disjoint support permutations). *If $\sigma_1, \sigma_2 \in S_n$ and $\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset$, then $\sigma_1\sigma_2 = \sigma_2\sigma_1$.*

Proof. Let $k \in \llbracket 1, n \rrbracket$.

If $k \notin \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$, then $\sigma_1\sigma_2(k) = k = \sigma_2\sigma_1(k)$

Without loss of generality, if $k \in \text{supp}(\sigma_1)$.


Then $k \notin \text{supp}(\sigma_2)$.

Thus $\sigma_1\sigma_2(k) = \sigma_1(k)$.

As $k \in \text{supp}(\sigma_1)$, $\sigma_1(k) \neq k$, thus $\sigma_1(\sigma_1(k)) \neq \sigma_1(k)$.

So $\sigma_1(k) \in \text{supp}(\sigma_1)$, thus $\sigma_1(k) \notin \text{supp}(\sigma_2)$.

Thus $\sigma_2\sigma_1(k) = \sigma_1(k) = \sigma_1\sigma_2(k)$.

In all cases, $\sigma_2\sigma_1(k) = \sigma_1\sigma_2(k)$, thus $\sigma_1\sigma_2 = \sigma_2\sigma_1$. 

Definition 8 (Length). *The length of $\sigma \in S_n$ is $\text{len}(\sigma) := \text{Card}(\text{supp}(\sigma))$.*

Theorem 2 (Length of a conjugation). *For all $\sigma_1, \sigma_2 \in S_n$, $\text{len}(\sigma_1\sigma_2) = \text{len}(\sigma_1)$.*

Proof. Let $k \in \llbracket 1, n \rrbracket$, let's proceed by case disjonction.

If $\sigma_2(k) \in \text{supp}(\sigma_1)$

Then $\sigma_1\sigma_2(k) \neq \sigma_2(k)$

Thus $\sigma_1\sigma_2(k) \neq k$

Thus $k \in \text{supp}(\sigma_1\sigma_2)$.

Otherwise $\sigma_2(k) \notin \text{supp}(\sigma_1)$

Then $\sigma_1\sigma_2(k) = \sigma_2(k)$

Thus $\sigma_{1\sigma_2}(k) = k$

Thus $k \notin \text{supp}(\sigma_{1\sigma_2})$.



It's very useful to build piece-wise solution to a cube and free-styling algorithms as it has (usually) small support and you choose with the σ_2 where the support will be.

The case of commutator is alike (although I don't see a clear formula for its length).

An example of switching only three corners in a rubik's cube is: $[[R, U], D]$ and 3 edges $[R_U, E]$ (where R, U, D, E are moves on a cube which will be explained later)

Definition 9 (Orbit). *Let $\sigma \in S_n$ and $i \in \llbracket 1, n \rrbracket$, the orbit is $\text{orb}_\sigma(i) := \{\sigma^k(i) | k \in \mathbb{N}\}$.*

Convention 4. *We'll write $\text{orb}(i)$ instead of $\text{orb}_\sigma(i)$ when which σ there are no confusion on which σ .*

Theorem 3 (Disjoint orbites). *Let $\sigma \in S_n$, then $\forall a, b \in \llbracket 1, n \rrbracket$, $\text{orb}(a) = \text{orb}(b) \vee \text{orb}(a) \cap \text{orb}(b) = \emptyset$.*

Proof. Let $\sigma \in S_n$.

Let $a, b \in \llbracket 1, n \rrbracket$

If $\text{orb}(a) \cap \text{orb}(b) \neq \emptyset$

Let $n \in \text{orb}(a) \cap \text{orb}(b)$.

Then there exist $k, j \in \mathbb{N}$ such that $n = \sigma^k(a) = \sigma^j(b)$.

Suppose without loss of generality that $k \geq j$.

Then $b = \sigma^{k-j}(a)$.

Thus

$$\begin{aligned} \text{orb}(b) &= \{\sigma^w(b) | w \in \mathbb{N}\} \\ &= \{\sigma^w(\sigma^{k-j}(a)) | w \in \mathbb{N}\} \\ &= \{\sigma^w(a) | w \in \mathbb{N} \setminus \llbracket 0, k-j-1, \rrbracket\} \\ &\subseteq \text{orb}(a) \end{aligned}$$

And conversely, let l be the smallest natural integer such that $\sigma^l(b) = \sigma^{k-j}(b)$.

Then $\sigma^l(b) = a$ and with same reasoning of before $\text{orb}(a) \subseteq \text{orb}(b)$.

Thus $\text{orb}(a) = \text{orb}(b)$



Definition 10 (Cycle). *We have $\sigma \in S_n$ a cycle if $\forall k \in \text{supp}(\sigma)$, $\text{orb}(k) = \text{supp}(\sigma)$.*

Notation 3 (Cycle). *Let $\sigma \in S_n$ be a cycle.*
if

$$\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_{\text{len}(\sigma)-1} & x_{\text{len}(\sigma)} \\ x_2 & x_3 & \dots & x_{\text{len}(\sigma)} & x_1 \end{pmatrix}$$

a reduced notation, then we can write σ as:

$$\sigma = (x_1 \ x_2 \ \dots \ x_{\text{len}(\sigma)})$$

The study of cycle is particularly important because:

Theorem 4 (Decomposition by cycles). *Let $\sigma \in S_n$, then $\exists! k \in \mathbb{N}, \exists! \{f_i \neq e \in$*

$$S_n \text{ cycle}\}_{i \in \llbracket 1, k \rrbracket}, \sigma = \prod_{i=1}^k f_i \wedge \forall i \neq j \in \llbracket 1, k \rrbracket, \text{orb}(f_i) \cap \text{orb}(f_j) = \emptyset$$

The abuse of notation of $\{f_i\}$ -ing is to indicate that the order of the f_i s doesn't matter, it is unique modulo f_i permutations.

Proof. Let $\sigma \in S_n$,

Unicity:

Let (f_i) and (g_i) all disjoint cycles such that $\sigma = \prod_1^k f_i = \prod_1^n g_i$.

Let $x \in \text{supp}(\sigma)$, then there are a f_i and g_j such that $\text{orb}_\sigma(x) = \text{supp}(f_i) = \text{supp}(g_j)$.

Thus $\forall n \in \mathbb{N}, f_i^n(x) = g_j^n(x)$.

Thus $f_i = g_j$.

And we can apply that logic on any $y \in \text{supp}(\sigma) \setminus \text{orb}_\sigma(x)$ until we match every f_i s and g_j s.


Existence:

Proof by giving an algorithm:

```

f ← []
S ← supp(σ)
while S ≠ ∅ do
  x ← min(S)
  R ← orbσ(x)
  S ← S \ R
  fi ← permutation with ∀w ∉ R, fi(w) = w ∧ fi(w) = σ(w)
  f ← f ∪ {fi}
end while
return f

```

This algorithm terminates and gives a correct (f_i) so it's true. 

Definition 11 (Order). *Let $\sigma \in S_n$, the order is $\text{ord}(\sigma) = \min(\{k \in \mathbb{N}^* | \sigma^k = e\})$*

Theorem 5 (Order of a permutation). *Let $\sigma \in S_n$ decomposed into disjoint cycles $(f_i)_{i \in \llbracket 1, k \rrbracket}$, then $\text{ord}(\sigma) = \text{lcm}(\text{ord}(f_1), \dots, \text{ord}(f_k))$.*

Proof. Let $l = \text{lcm}(\text{ord}(f_1), \dots, \text{ord}(f_k))$.

Then

$$\begin{aligned}
\sigma^l &= (f_1 \dots f_k)^l \\
&= f_1^l \dots f_k^l \\
&= e \dots e \\
&= e
\end{aligned}$$



Thus $\text{ord}(\sigma) \leq l$.

Let's prove that $\forall x \in \llbracket 1, l-1 \rrbracket, \sigma^x \neq e$.

Let $x \in \llbracket 1, l-1 \rrbracket$,

Then

$$\begin{aligned}
\sigma^x &= (f_1 \dots f_k)^x \\
&= f_1^x \dots f_k^x
\end{aligned}$$

But one of the $f_i^x \neq e$ (otherwise l isn't the lcm).

Thus $\sigma^x \neq e$.

Thus $\text{ord}(\sigma) \geq l$.

We have $l \leq \text{ord}(\sigma) \leq l$.

Thus $\text{ord}(\sigma) = l$.

Definition 12 (Inversion). *Let $\sigma \in S_n$ and $i, j \in \llbracket 1, n \rrbracket$ with $i < j$. We say that (i, j) is an inversion under σ if $\sigma(i) > \sigma(j)$.*

Definition 13 (Signature). *The signature of $\sigma \in S_n$ is $(-1)^k$ where k is the number of inversions. And is noted $\epsilon(\sigma)$ and is equal to $\prod_{i,j \in \llbracket 1, n \rrbracket : i < j} \frac{\sigma(i) - \sigma(j)}{i - j}$.*

Theorem 6 (Signature is a morphism). *For all $\sigma, \tau \in S_n$, $\epsilon(\tau\sigma) = \epsilon(\tau)\epsilon(\sigma)$.*

Proof. Let $\sigma, \tau \in S_n$,

We have

$$\begin{aligned}
\prod_{i,j \in \llbracket 1, n \rrbracket : i < j} \frac{\tau\sigma(i) - \tau\sigma(j)}{i - j} &= \prod_{i,j \in \llbracket 1, n \rrbracket : i < j} \frac{\tau(i) - \tau(j)}{\sigma^{-1}(i) - \sigma^{-1}(j)} \\
&= \prod_{i,j \in \llbracket 1, n \rrbracket : i < j} \frac{\tau(i) - \tau(j)}{i - j} \prod_{i,j \in \llbracket 1, n \rrbracket : i < j} \frac{i - j}{\sigma^{-1}(i) - \sigma^{-1}(j)} \\
&= \prod_{i,j \in \llbracket 1, n \rrbracket : i < j} \frac{\tau(i) - \tau(j)}{i - j} \prod_{i,j \in \llbracket 1, n \rrbracket : i < j} \frac{\sigma(i) - \sigma(j)}{i - j} \\
&= \epsilon(\tau)\epsilon(\sigma)
\end{aligned}$$



Theorem 7 (Signature of a cycle). *Let $\sigma \in S_n$ be a cycle, then $\epsilon(\sigma) = (-1)^{1+\text{len}(\sigma)}$.*

Proof. Let $\sigma \in S_n$ be a cycle.

Let's write $(x_1 \ x_2 \ \dots \ x_{\text{len}(\sigma)}) := \sigma$.

Then

$$\begin{aligned}
 \epsilon(\sigma) &= \epsilon((x_1 \ x_2 \ \dots \ x_{\text{len}(\sigma)})) \\
 &= \epsilon\left(\prod_{i=1}^{\text{len}(\sigma)-1} (x_{\text{len}(\sigma)-i+1} \ x_{\text{len}(\sigma)-i})\right) \\
 &= \prod_{i=1}^{\text{len}(\sigma)-1} \epsilon((x_{\text{len}(\sigma)-i+1} \ x_{\text{len}(\sigma)-i})) \\
 &= \prod_{i=1}^{\text{len}(\sigma)-1} -1 \\
 &= (-1)^{\text{len}(\sigma)-1} \\
 &= (-1)^{\text{len}(\sigma)+1}
 \end{aligned}$$



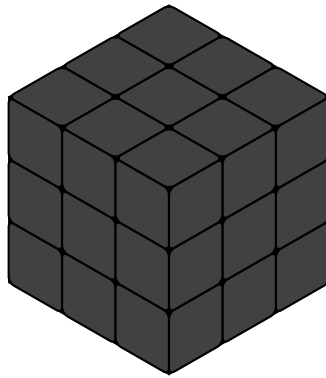
2 Topology of a rubik's cube

2.1 Pieces of the cube

We won't consider the cube as being a combinaison of stickers (colors) on 6 different faces.

Although it is one of the easiest (most intuitive) way for beginners, this view isn't powerful enough for me to still be able to explain the topology of a cube.

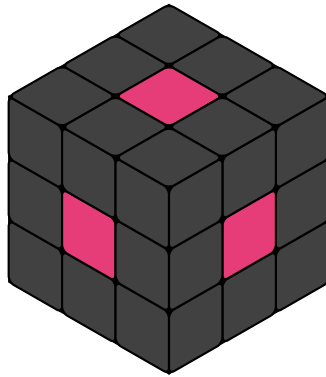
We'll think of it as being pieces, a piece being a 1×1 smaller cube which compose the rubik's cube.



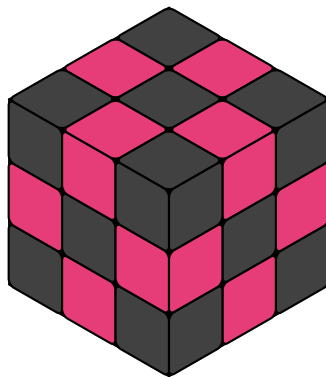
The entire cube is made of 27 pieces, though the one enclosed by the others isn't important (we don't see it), so we'll consider that we have 26.

I'll distinguish 3 types of pieces.

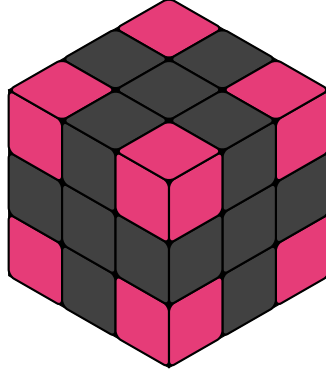
There are the 6 centers, which touch exactly 1 face:



There are the 12 edges, which touch exactly 2 faces:



And finally the 8 corners, which touch exactly 3 faces:



Some could argue that centers aren't pieces as they don't move, I'll consider that they do move as it'll make the rest of this article easier (more consistent convention, it'll be clear later).

Thus, when speaking about a cube, for now I'll speak about the combination of the three type of pieces.

2.2 State as a permutation

Definition 14 (Color of a face). *The color of a face is the color of its center piece.*

Convention 5. *I'll say "(color) face" to refer to "the face of the cube with color (color)"*

Unicity will be proved later.

Definition 15 (Solved cube). *A solved cube is one with all faces having only 1 color, with green in front and yellow on top, we'll keep calling it e .*

An experienced cuber will find the faces position condition weird, but it's important to later on decide on what is the neutral element of a cube (when seen as a permutation subgroup).

Definition 16 (Valid state of a cube). *A valid state of a cube is one that is achievable from doing valid moves from the solved cube.*

The notion of "valid moves" will be explained later.

Definition 17 (Moves of a state). *If S is a valid state, we denote by $\text{moves}(S)$ any finite moves sequence which when applied to e sequentially, gives S .*

The existence of finiteness of move sequence

We'll now speak about S and $\text{moves}(S)$ as if they are the same, and the states as a group by defining ab be the state when applying $\text{moves}(a)$ then $\text{moves}(b)$ to e .

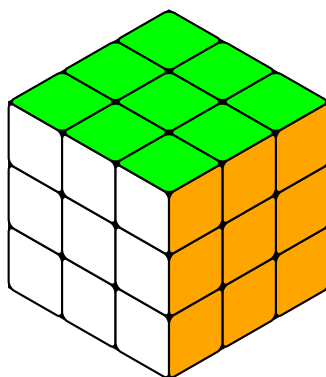
2.3 Moves, algorithms and notations

Definition 18 (Algorithm). *An algorithm is a sequence of moves, generally to achieve a certain outcome.*

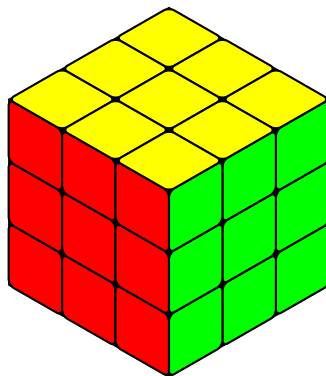
I'll differentiate two kind of moves, rotations and turns.

2.3.1 Rotations

Rotations are moves which can be done on a 1×1 , there are done on 3 axis:
The x rotation, which put the front face into the top and bottom into the front:



The y rotation, which put the front face into the right and left into the front:



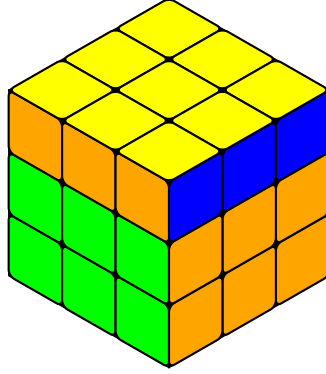
And finally the z rotation, which put the top face to the right and the right face at the bottom, and we have $z = x^{-1}y^{-1}x = y^{-1}_{x^{-1}}$ (we apply from left to right, that's why it's $y^{-1}_{x^{-1}}$ instead of y^{-1}_x)

2.3.2 Turns

A turn is a move which cannot be done on a 1×1 as they turn part of the cube.

There are the moves U, D, R, L, F, B alongside their wide counterpart: u, d, r, l, f, b ; and the slices moves M, E, S .

All comes from the U (up) and some rotations, you turn the upper layer clockwise:



And now define :

- (down) $D = U_{x^2}$
- (front) $F = U_x$
- (back) $B = U_{x^{-1}}$
- (right) $R = U_{z^{-1}}$
- (left) $L = U_z$

And $u = Dy$ and defining the d, f, b, r, l as

- (down) $d = u_{x^2}$
- (front) $f = u_x$
- (back) $b = u_{x^{-1}}$
- (right) $r = u_{z^{-1}}$
- (left) $l = u_z$

And finally, the three last turns I'll use

- $M = RL^{-1}x^{-1}$
- $E = DU^{-1}y^{-1}$
- $S = BF^{-1}z$

It's a lot of notation but it's easy to learn, take a cube and try them or look at them online.

Which means that the states of a cube is $\langle U, x, y \rangle$.

If we don't allow ourselves moves which modify the center, the states of a cube is $\langle U, D, F, B, L, R \rangle = \langle U, F, B, L, R \rangle$ because $D = (U_{(U^2 R^2)^3})_{F^2 R^2 L^2 B^2}$, a further examination of the cube will show that rotationless, it is not generated with only 4 moves.

It we'll show later that the states of rotationless rubik's cube can be generated with two rotationless algorithms.

2.4 Centers

There are 6 centers. The white, yellow, red, green and blue ones.

We'll now demonstrate that their placement is uniquely determined by the front and up centers.

Theorem 8 (Opposite centers). *If centers A and B are on the antipodes in e , then they are in any state.*

Proof. Remember, the states are $\langle U, x, y \rangle$, and U doesn't modify the centers.

So we need to prove that this property holds after doing x and after doing y .

Without loss of generality, let's suppose that A is in left or up or front.

If A in front, then y doesn't affect A and B and x puts them on up and bottom so still opposite.

If A in up, then x put A and B on back and front and y puts them on right and left so still opposite.

Lastly, if A is left, x doesn't affect A and B and y puts them on up and bottom so still opposite. 🧐

Theorem 9 (Adjacent centers). *If A, B, C are 2-by-2 adjacent centers such that $A \rightarrow B \rightarrow C \rightarrow A$ from outside the cube do a clockwise motion, after any rotations it stays as so.*

Proof. From the opposite centers, they all are still 2-by-2 adjacent.

Doing the $6 \times 5 \times 2$ cases disjunction is too long for this paper, do it if you want, but I'll assume peoples living in a 3D world can intuition it to be true. 🧐

All that to prove that the centers are unique and doesn't move around compared to the others, so they are uniquely determined by the position of two adjacent centers, so there are 6×4 possible center positions (which are all accessible).

2.5 Edges

Theorem 10 (Unicity of edges). *If A and B are adjacent colored faces, then there exists an unique edge of both those colors.*

Proof. True for a solved cube, x and y obviously doesn't change that and neither does U . 🧐

Definition 19 (Edge orientation). *We define two state of an edge, "good" and "bad" orientation. Bad orientation is when it is not good and good is one that can be inserted into the right place matching the right colors by a state of $\langle U, D, R, L \rangle$. We'll say "oriented" instead of "good" oriented and "misoriented" instead of "bad" oriented. And we define the function for E an edge,*

$$\text{orientation}(E) = \begin{cases} 0 & \text{if } E \text{ is well oriented} \\ 1 & \text{if } E \text{ is misoriented} \end{cases}$$

Proof. I'll only consider the case of the edge being in front-top and front-right as others are symmetries.

If the edge is on front-top, doing FRU will place it on the same spot, but with a different orientation, so its orientation changed.

If the edge is on front-right, doing FDR will place it on the same spot, but with a different orientation, so its orientation changed. 🧐

Theorem 11 (Edge orientation changer). *An edge on the front (resp. back) change orientation when doing an F (resp. B) move.*

That means that rotationless cube isn't generated with only 4 of U, D, L, R, F, B as it either can't change orientation or can't access an edge.

Theorem 12 (Edge orientation parity). *The possible edge orientations of a cube are exactly those with $\sum_{E \in \text{edges}} \text{orientation}(E) \equiv 0 \pmod{2}$, and it is independent on the placement of other pieces.*

Proof. By doing an F (or B), you change the orientation of 4 edges.

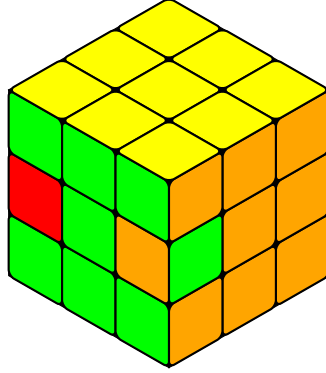
If they are all oriented, then they are all misoriented, so same number modulo 2.

If there are 3 oriented (and one misoriented), then there are 3 misoriented and one oriented, so same number modulo 2.

Same for 2 and 1 and 0 oriented edges.

So the number of misoriented edges on all states is even.

The state $[[R, U]U_{F^{-1}}, E^{-1}]$ is:



With exactly the front-left and front-right edges being misoriented.
 So with some conjugation on $[[R, U]U_{F^{-1}}, E^{-1}]$ you can misorient any two pieces.
 So by applying it multiple times, you can misorient any even number of pieces independently of the placement of other pieces.



2.6 Corners

Theorem 13 (Unicity of corners). *If A , B and C are 2-by-2 adjacent colors, then there exists a unique corner of those colors with same way of $A \rightarrow B \rightarrow C \rightarrow A$ (clockwise or counter-clockwise).*

Proof. Neither U , x nor y changes this and it's trivial on a solved cube.



Definition 20 (Orientation of a corner). *Let C be a corner, it must have one of its color being of the top or bottom face.
 We say that it is*

- *Well oriented if that color is facing the top or bottom*
- *Needing a clockwise turn if a clockwise turn of the corner (not a valid cubing move) will bring that color to the top or bottom*
- *Needing a counter-clockwise turn if a counter-clockwise turn of the corner (not a valid cubing move) will bring that color to the top or bottom*

And we define the function

$$\text{orientation}(C) = \begin{cases} 0 & \text{if } C \text{ is well oriented} \\ 1 & \text{if } C \text{ needs a clockwise turn} \\ -1 & \text{if } C \text{ needs a counter-clockwise turn} \end{cases}$$

Theorem 14 (Corner orientation parity). *Possible orientations of corners of valid states are exactly those where $\sum_{c \in \text{corners}} \text{orientation}(c) \equiv 0 \pmod{3}$.*

Proof. We have $\sum_{c \in \text{corners}} \text{orientation}(c) \equiv 0 \pmod 3$ for a solved cube.

As the rotations, with respect to only corners, can be done without rotations and only turns, I'll only analyse turns.

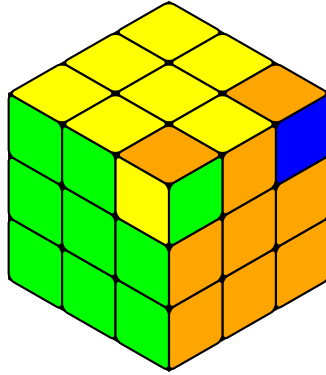
We have U and D which doesn't change orientation of corners.

We have F , B , R and L which turns 2 corners clockwise and two counter clockwise.

So for any valid state, $\sum_{c \in \text{corners}} \text{orientation}(c) \equiv 0 \pmod 3$.

Now let's prove that if we have a valid state, we can modify its corners orientations as long as $\sum_{c \in \text{corners}} \text{orientation}(c) \equiv 0 \pmod 3$.

Let's consider the algorithm $[[R^{-1}, D^{-1}]^2, U]$:



It do a clockwise turn to the top-right-back corner and counter-clockwise to the top-right-front corners without any other modifications.

So by conjugating it and using the top-right-back as a buffer, as long as it's from a valid state, any subsequent permutations differing only in corner orientation and respecting $\sum_{c \in \text{corners}} \text{orientation}(c) \equiv 0 \pmod 3$ is possible. 🤖

2.7 Valid state

We already know of a valid state should behave in term of its orientations, but what about the position of the pieces (without regard to orientation) ?

For that, we'll now consider the cube as being orientationless.

For now, let's also consider the cube to be rotationless.

Theorem 15 (Edge-corner parity). *If S is a rotationless, orientationless state, then $\epsilon(S) = 1$.*

Proof. Obvious for the solved cube.

Let $W = U$ or D or F or B or R or L .

We have W which modify 4 centers and 4 edges.

And those edges/centers both do a length 4 cycle, so with signature -1 .

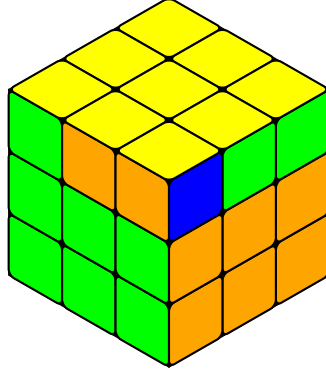
So $\epsilon(W) = -1 \times -1 = 1$. 🤖

Theorem 16 (Edge-corner parity completeness). *If S is a permutation of a rotationless and orientationless cube (mapping centers to centers and edges to edges, not touching centers), S is a state if and only if $\epsilon(S) = 1$.*

Proof. One side of the equivalence has already been proven.

So now let's prove that any permutation P with $\epsilon(P) = 1$ "making sense" (transform a cube into a cube) of an orientationless and rotationless cube is a state, aka. that it is constructible.

For that, we'll consider the state (called "J-perm"), $U_R F[R, U] F_{R^{-1}} U^{-1} R U^{-1}$:



Swap exactly two edges and two corners, and by doing conjugate without changing the corners you can place the edges as you want and by doing conjugate without changing those edges you can then place the corners as you want (as long as they satisfy the edges-corners parity). 🧐

Theorem 17 (Edge-corner-center parity). *Even for when accounting center movement, the valid state of a orientationless cube are exactly those with: $\epsilon(S) = 1$.*

Proof. We have $\epsilon(x) = \epsilon(y) = 1$.

so we can do some rotation and then go to a permutation that have an 1 for signature with only rotationless moves. 🧐

So, we can consider a state S as a tuple p, o with $S = o \circ p$ with o only changing orientation respecting edges and corners orientations parity and p not changing any orientation respecting the center-edge-corners parity and vice versa, $o \circ p$ for any o and p will give a valid state.

2.8 Order of rubik's cube permutations

Now that we can define exactly the valid states of a cube based on some easy to check criteria, we can say some more interesting things.

Theorem 18 (The rotationless cube is 2-generated). *There exist two state, α and β such that the rotationless cube is $\langle \alpha, \beta \rangle$.*

Proof. We just chose any α and β having those properties:

α doesn't change orientation, but do a 7 corner and 11 edge cycle.

And β do a 2 corner swap including the one untouched by α changing the orientation of one and changing the orientation of a non-moving (under β) corner, and a 2 edge swap changing the orientation of one and of a non-moving (under β) edge.

Note that β^2 doesn't change position of pieces, it only change the orientation of two edges and 3 corners, thus β^4 only changes the orientation of 3 corners and β^6 only change the orientation of 2 edges.

Note that α^7 is an edge cycle and α^{11} is a corner cycle.

We can place all pieces at the right spot (but not necessarily with the right orientation) by first creating cycles of corners with α^{11} and β using the untouched corner of α as a buffer, and then doing the same for edges with β and α^7 .


We'll now orient them all one by one.

Starting with edges, by conjugation you can put two misoriented edges into the support of β^6 and reverse the setup move, so we can orient any edges.


Now for the corners, still by conjugation, as long as there are ≥ 3 misoriented corners, you can orient them one by one with conjugation of β^4 .

Now, if there are still 2 misoriented corners left, you can solve one of them and put two oriented one to the support of β^4 .

Now, you have 3 misoriented corners, and applying β^4 on them multiple time will solve them.

So we can solve any rotationless states, thus by reversing them moves, any state is achievable by α and β only. 

Theorem 19 (Number of permutation of a cube). *A rotationless cube as $\frac{3^8 \times 8! \times 12! \times 2^{12}}{2 \times 2 \times 3} = 43\,252\,003\,274\,489\,856\,000$ permutations, and a cube including rotation as $\frac{6 \times 4 \times 3^8 \times 8! \times 12! \times 2^{12}}{2 \times 2 \times 3} = 1\,038\,048\,078\,587\,756\,544\,000$ permutations.*

Proof. Direct by counting the number of placement and orientation while accounting for parities. 

Theorem 20. *If S is a state and $\text{ord}(S) = a \times b$ with $\gcd(a, b) = 1$, then there exist A and B states such that $\text{ord}(A) = a$ and $\text{ord}(B) = b$.*

Proof. Let $A = S^b$ and $B = S^a$.

We'll now prove that $\text{ord}(A) = a$ and that $\text{ord}(B) = b$.

We'll only prove that $\text{ord}(A) = a$ as the B case is just a proof symmetry and is obtained similarly.

Let's decompose S into cycles (s_1, s_2, \dots, s_n) , we know that $\text{lcm}_{i=1}^n \text{ord}(s_i) = \text{ord}(S) = a \times b$.

Thus $\text{lcm}_{i=1}^n \text{ord}(s_i^b) = \text{ord}(S^b) = \text{ord}(A)$.

For each s_i , it is obvious that $\text{ord}(s_i^b) \mid \text{ord}(s_i)$, thus $\text{ord}(A) \mid a \times b$.

And for each s_i , if $\text{ord}(s_i) \mid b$, we have $\text{ord}(s_i) = 1$.

Thus $\text{ord}(A) \mid a$.

And for each s_i such that $\neg(\text{ord}(s_i) \mid b)$, we can write $a'b' := \text{ord}(s_i)$ with $\gcd(a', b) = 1 = \gcd(a, b')$, and thus $\text{ord}(s_i) = a'$.

Thus $a \mid \text{ord}(A)$.

Thus $a = \text{ord}(A)$.



Theorem 21 (Form of a cube ordinal). *If S is a state, then there exists $a, b, c, d, e \in \mathbb{N}$ such that $\text{ord}(S) = 2^a 3^b 5^c 7^d 11^e$.*

Proof. Let $p > 11$ be prime.

Let's try to do a state of order p and show that it's not possible.

If we want to make one, it must be constituted one or multiple cycles of order exactly p .

It is not possible by doing orientations (edge orientation changes would assure that $2 \mid p$ which isn't the case and corner would assure that $3 \mid p$).

It is not possible by doing permutation of centers, nor of corners, nor of edges (not enough pieces).

Thus doing a $\text{ord}(S) = p$ isn't possible, and it comes from the previous theorem that there are no S state such that $p \mid \text{ord}(S)$.



For some example: $\text{ord}(e) = 1$, $\text{ord}(R^2) = 2$, $\text{ord}([R^{-1}, D^{-1}]^2, U) = 3$, $\text{ord}(U) = 4$, any 5 cycle without changing orientation as $\text{ord } 5$, $\text{ord}([R, U]) = 6$, $\text{ord}(RU^{-1}F^{-1}U) = 7$, orientationless permutation of all cycle as $\text{ord } 8$, 9 orientationless edge cycle has $\text{ord } 9$, 5-edge cycle and 2 changing orientation has $\text{ord } 10$, 11 orientationless edge cycle has $\text{ord } 11$, etc.

Theorem 22 (Longest cube ordinal). *The longest cube ordinal as for ordinal : $2 \times 3 \times 7 \times 11 = 462$.*

Proof. Let A be one of the state with maximum ordinal.

We first observe that if p is a orientationless cycle, then by misorienting an edge, if $\text{ord}(p)$ is odd, will multiply $\text{ord}(p)$ by 2, otherwise does nothing.

Same for changing orientation on corners, if $\text{ord}(p)$ isn't a multiple of 3, it multiplies $\text{ord}(p)$ by 3, otherwise does nothing.

So let's assume without loss of generality that A has an edge and a corner orientating changer.

So we know that $6 \mid A$ even without considering pieces placement.

As the center placement are cycles of length 1, 2 or 3, they won't change the $\text{ord}(A)$, so we will choose whatever is convenient for the edge-corner-center parity.

If the center permutation as a negative signature:


Either one of the corners or edge will need to have at least one even cycle, which is obviously inefficient.

Thus the center permutation as a positive signature.


Choosing cycles of even length or multiple by 3 is obviously suboptimal, thus the combinaison to consider are (format: (center cycle length ; edge cycle length)):

- (5 ; 5 7)
- (7 ; 5 7)

- $(7 ; 11)$

And the maximum ordinal is obtained by $(7; 11)$, thus the longest cube ordinal is $2 \times 3 \times 7 \times 11$. 

Theorem 23 (The cube is not 1-generated). *There are no state S such that the cube is $\langle S \rangle$.*

Proof. First proof, all state have way too small ordinal. 

Proof. Second proof, let's do it by absurd.

Let's suppose that there are S such that the cube is $\langle S \rangle$.

Then there exist $a, b \in \mathbb{N}$ such that $U = S^a$ and $R = S^b$.

Thus $RU = S^a S^b = S^{a+b} = S^b S^a = UR$.

Though, $RU \neq UR$, so our assumption was false, thus there exist no such S . 