Rubik's Cube – How to Come Up With a Solution?

Tsz-Wo Sze

$2025 \cdot 8 \cdot 31$

Abstract

Rubik's Cube can be considered as a permutation group, a.k.a. the *Rubik's Cube group*. We discuss some ideas for solving it. Our intention is not to give out a complete solution – we only provide ideas and offer inspiration encouraging the readers to come up with a solution on their own.

1 Introduction to Groups & Permutations

In this section, we give a very brief introduction to groups and permutations.

1.1 Groups

Definition (Groups)**.** A *group* $(G, *)$ consists of a set G and an operator $*$ satisfying the followings.

1. *Closure*: for any $g_1, g_2 \in G$, $g_1 * g_2 \in G$.
2. *Associativity*: for any $g_1, g_2, g_3 \in G$, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.
3. *Identity*: there exists $e \in G$, namely the *identity* element, such that $e * g = g * e = g$ for any $g \in G$.
4. *Inverses*: for any $g \in G$, there exists $h \in G$, namely the *inverse* of g, such that $g * h = h * g = e$.

When $(G, *)$ satisfies the additional property below, it is called a *commutative* group or an *abelian* group.

- *Commutativity*: for any $g_1, g_2 \in G$, $g_1 * g_2 = g_2 * g_1$.

Example 1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{x>0}, \times)$ are groups but $(\mathbb{Z}_{n\geq 0}, +)$, $(\mathbb{Z}_{n>0}, \times)$ and $(\mathbb{Q}, \times)$ are not.

Definition (Subgroups)**.** Let $(G, *)$, $(H, *)$ be groups, where $H \subset G$. Then $(H, *)$ is a *subgroup* of $(G, *)$.

From now on, we drop the operator symbol $*$ and denote the group operation as multiplication: the group $(G, *)$, the group operation $g_1 * g_2$ and the inverse of g are denoted by G, $g_1 g_2$ and g^{-1}, respectively.

Definition (Commute)**.** Let G be a group and $g_1, g_2 \in G$, if $g_1 g_2 = g_2 g_1$, then g_1 and g_2 *commute*.

Definition (Order)**.** Let G be a finite set. The *order* of the group G is defined to be $|G|$, the size of the set G. For any $g \in G$, the *order* of g is defined to be d, where $g^d = e$ and $g^i \neq e$ for $0 < i < d$.

Definition (Commutators)**.** Let G be a group. For any $g, h \in G$, the *commutator* $[h, g]$ is $h^{-1}g^{-1}hg$.

Definition (Conjugates)**.** Let G be a group. For any $g, h \in G$, the *conjugate* of g by h is hgh^{-1}.

Definition (Generator Set)**.** Let G be a finite group and $\mathcal{G} := \{g_1, \ldots, g_m\}$ be a subset of G. Then, $H := \{g \in G \mid g \text{ is a finite product of } g_1, \ldots, g_m\}$ is a subgroup of G and $\mathcal{G}$ is a *generator set* of H.

Lemma 1 (Inverses)**.** *Let G be group and $g := g_1 g_2 \cdots g_m$ for any $g_1, \ldots, g_m \in G$. Then $g^{-1} = g_m^{-1} \cdots g_2^{-1} g_1^{-1}$. Consequently, for any $g, h \in G$, $[h, g]^{-1} = [g, h]$ and $C_h(g)^{-1} = C_h(g^{-1})$, where $C_h(x) := hxh^{-1}$ is the conjugate-by-h function.*

1.2 Permutations

Let $N := \{1, \ldots, n\}$ be a set of n integers and $\mathcal{S}_n$ be the set of permutations over N.

Definition (Permutations)**.** A *permutation* σ is a bijective function $\sigma : N \to N$.

Definition (Cycles & Transpositions)**.** A permutation σ with order d mapping d distinct elements in a cycle and preserving the remaining elements is called an *order d cycle*, an *d-cycle* or simply a *cycle*. An *d-cycle* is denoted by $\sigma := \begin{pmatrix} a_1 & \ldots & a_d \end{pmatrix}$, where $\sigma(a_i) = a_{i+1}$ for $1 \leq i < d$ and $\sigma(a_d) = a_1$.

A permutation swapping only two elements, which is a 2-cycle, is called a *transposition*.

Definition (Symmetric Groups)**.** The set $\mathcal{S}_n$ together with the operator $\circ$ is a group, called the *symmetric group of degree* n, where $\circ$ is the function composition operator

$$\tau \circ \sigma : N \longrightarrow N, \qquad (\tau \circ \sigma)(a) := \tau(\sigma(a)) \qquad \text{for any } \sigma, \tau \in \mathcal{S}_n \text{ and any } a \in N.$$

Definition (Permutation Groups)**.** A subgroup $\mathcal{P} \subset \mathcal{S}_n$ is called a *permutation group*.

Lemma 2 (3-Cycles & Transpositions)**.** *An order 3 cycle is the same as two transpositions*

$$\begin{pmatrix} a & b & c \end{pmatrix} \quad = \quad \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} b & c \end{pmatrix} \qquad \left(\neq \begin{pmatrix} b & c \end{pmatrix}\begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} a & c & b \end{pmatrix}\right). \tag{1}$$

Lemma 3 (Commutativity of $\mathcal{S}_n$)**.** *The group $\mathcal{S}_n$ is commutative if and only if $n \leq 2$.*

Proof. It is obvious that $\mathcal{S}_1$ and $\mathcal{S}_2$ are commutative. For $n > 2$, the set N has at least 3 elements. The group $\mathcal{S}_n$ is non-commutative since $\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} b & c \end{pmatrix} \neq \begin{pmatrix} b & c \end{pmatrix}\begin{pmatrix} a & b \end{pmatrix}$ as in equation (1). □

Lemma 4 (Cycle Decomposition)**.** *Any permutation $\sigma : N \to N$ can be decomposed into disjoint cycles. Disjoint cycles commute with each other. The order of σ is the least common multiple of the orders of the cycles. An d-cycle in σ becomes the identity in σ^d. An (mk)-cycle in σ becomes k order m cycles in σ^k.*

Lemma 5 (Conjugate Permutations)**.** *Let τ be any permutation. Let $\sigma := \begin{pmatrix} a_1 & \dots & a_m \end{pmatrix}$ be an m-cycle. The conjugate of σ by τ is*

$$\tau\sigma\tau^{-1} \quad = \quad \begin{pmatrix} \tau(a_1) & \dots & \tau(a_m) \end{pmatrix}.$$

Let $\sigma_1, \dots, \sigma_k$ be k disjoint cycles, where $\sigma_i := \begin{pmatrix} a_{i,1} & \dots & a_{i,m_i} \end{pmatrix}$ is an m_i-cycle. The conjugate of $\sigma_1 \dots \sigma_k$ by τ is

$$\tau(\sigma_1 \dots \sigma_k)\tau^{-1} \quad = \quad \begin{pmatrix} \tau(a_{1,1}) & \dots & \tau(a_{1,m_1}) \end{pmatrix} \cdots \begin{pmatrix} \tau(a_{k,1}) & \dots & \tau(a_{k,m_k}) \end{pmatrix}.$$

Proof. For the first part, let $a_{m+1} := a_1$ and $\sigma_\tau := \begin{pmatrix} \tau(a_1) & \dots & \tau(a_m) \end{pmatrix}$. For any $b \in N$, let $x := \tau^{-1}(b)$. If $x = a_j$ for some $1 \leq j \leq m$, then $\tau(a_j) = b$. We have

$$\tau\sigma\tau^{-1}(b) \quad = \quad \tau\sigma(a_j) \quad = \quad \tau(a_{j+1}) \quad = \quad \sigma_\tau(\tau(a_j)) \quad = \quad \sigma_\tau(b).$$

Otherwise, $\tau^{-1}(b) = x \neq a_j$ and $b \neq \tau(a_j)$ for any $1 \leq j \leq m$, then $\sigma(x) = x$ and $\sigma_\tau(b) = b$. We have

$$\tau\sigma\tau^{-1}(b) \quad = \quad \tau\sigma(x) \quad = \quad \tau(x) \quad = \quad b \quad = \quad \sigma_\tau(b).$$

The second part is trivial since $\tau(\sigma_1 \dots \sigma_k)\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_k\tau^{-1})$. □

Example 2. Let $\sigma \in \mathcal{S}_6$ such that $\sigma(1) = 4, \sigma(2) = 3, \sigma(3) = 2, \sigma(4) = 6, \sigma(5) = 5, \sigma(6) = 1$. Then,

$$\sigma \quad = \quad \begin{pmatrix} 1 & 4 & 6 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 5 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 4 & 6 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}.$$

Since the cycles of σ have different orders, we may apply σ repeatedly in order to preserve some of the elements: $\sigma^2 = \begin{pmatrix} 1 & 6 & 4 \end{pmatrix}$ preserves 2 and 3; $\sigma^3 = \begin{pmatrix} 2 & 3 \end{pmatrix}$ preserves 1, 4 and 6; and σ^6 is the identity.

Let $\tau := \begin{pmatrix} 1 & 2 & 5 \end{pmatrix}$. The conjugate of σ by τ is $\tau\sigma\tau^{-1} = \begin{pmatrix} 2 & 4 & 6 \end{pmatrix}\begin{pmatrix} 5 & 3 \end{pmatrix}$ by Lemma 5.

2 Rubik's Cube

A Rubik's Cube has 6 faces with different colors and each colored face has 9 squares (a center, 4 corners and 4 edges) in the same color. We use Singmaster's notation naming the faces front (f), back (b), left (ℓ), right (r), up (u) and down (d). Each face can be rotated clockwise or anti-clockwise. In the table below, we use upper case letters to denote the clockwise rotation moves when looking toward to the faces.

Faces	front (f)	back (b)	left (ℓ)	right (r)	up (u)	down (d)
90° clockwise	F	B	L	R	U	D
90° anit-clockwise	F^{-1}	B^{-1}	L^{-1}	R^{-1}	U^{-1}	D^{-1}

One may also consider the moves of fixing two opposite faces and rotating the middle layer in between. For example, we may rotate the middle layer between f and b. Such move is the same as rotating both f and b in the reversing direction. For simplicity, we ignore all the middle layer moves. As a result, the position of the center square in each face remains unchanged for any moves.

The following is a sequence of 4 moves

$$U, \quad F^{-1}, \quad U^{-1}, \quad F.$$

The sequence is applied from left to right. When the moves are written as a function composition

$$M := FU^{-1}F^{-1}U, \qquad M(\alpha) = F(U^{-1}(F^{-1}(U(\alpha)))) \tag{2}$$

the functions are applied from right to left. The inverse is just reversing all the moves (Lemma 1), i.e.

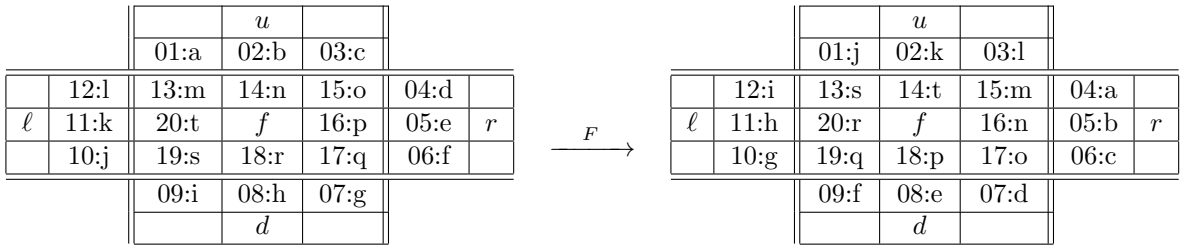
$$M^{-1} \quad = \quad (FU^{-1}F^{-1}U)^{-1} \quad = \quad U^{-1}FUF^{-1}.$$

2.1 Rubik's Cube as a Permutation Group

A Rubik's cube has 48 non-center squares. A sequence of moves is a permutation of these squares. Let $\mathcal{P}$ be the set of sequences of moves and $\mathcal{G} := \{F, B, L, R, U, D\}$. Then, $\mathcal{P}$ is a permutation group, a subgroup of the symmetric group $\mathcal{S}_{48}$ called the *Rubik's cube group*, and $\mathcal{G}$ is a generator set of $\mathcal{P}$.

In the initial configuration α_0 of Figure 1, the squares on f and the surrounding squares are numbered from 01 to 20, and a letter is assigned to each square. The numbers are the "addresses" and letters are the "contents". The configuration α_F is obtained by applying F to each square in α_0. The permutation F is decomposed into 5 disjoint 4-cycles $F_1, \ldots, F_5$, where F_2, F_5 map edges to edges and F_1, F_3, F_4 map corners to corners. In general, the permutations in $\mathcal{P}$ map edges to edges, corners to corners.

$$F := F_1F_2F_3F_4F_5, \qquad \textit{where} \quad F_1 := (01\ \ 04\ \ 07\ \ 10), \qquad F_2 := (02\ \ 05\ \ 08\ \ 11),$$
$$F_3 := (03\ \ 06\ \ 09\ \ 12), \qquad F_4 := (13\ \ 15\ \ 17\ \ 19),$$
$$F_5 := (14\ \ 16\ \ 18\ \ 20).$$



α_0: Initial configuration $\qquad$ $\alpha_F := F(\alpha_0)$

Figure 1: Applying F to α_0

Solving Rubik's cube is not easy. One reason is that each permutation in $\mathcal{G}$ moves many squares at once. If there are ways to move fewer squares, it becomes possible to solve the cube bit by bit.

Idea 0 (Basic Idea: The Fewer The Better)**.** *Find some ways to move fewer squares.*

2.2 Cycle Decomposition

If a permutation can be decomposed into cycles with different orders, it can be applied repeatedly until fewer squares are moved as in Example 2. In equation (2), M indeed is the commutator $[F^{-1}, U]$ which moves 12 corners, 6 edges and preserves the remaining 12 corners, 18 edges. The cycle decomposition of M has two order 3 edge cycles and two order 6 corner cycles. By Lemma 4, the order of M is 6. Let

$$T := M^3 = [F^{-1}, U]^3 = (FU^{-1}F^{-1}U)^3. \tag{3}$$

Then, T consists of 6 transpositions since the two order 3 edge cycles becomes the identity and the two order 6 corner cycles becomes six 2-cycles. The permutation T preserves all the edges and moves fewer squares than M. Similarly, M^2 consists of six 3-cycles – two edge cycles and four corner cycles.

Idea 1 (Think Cycle Decomposition)**.** *Any permutation $\sigma \in \mathcal{P}$ has a finite order. Suppose σ has cycles in different orders. By Lemma 4, σ^d which eliminates the d-cycles in σ, moves fewer squares (Idea 0).*

Idea 2 (Edges First or Corners First)**.** *Since there are edge preserving permutations (e.g. T in equation (3)) which moves only the corners but not the edges, we may*

1. *solve all the edges by ignoring the corners; and then*
2. *solve the corners by the edge preserving permutations.*

Alternatively, we may solve the corners first and then the edges using corner preserving permutations.

2.3 Conjugates

After played Rubik's cube for some time, we may come up with some sequences of moves to perform useful permutations. In practice, the actual squares may not be positioned in the way that a particular permutation σ can be applied. We may try to find a conjugate of σ by another permutation $\tau \in \mathcal{P}$. The meaning of "conjugate by τ" is the strategy which (1) uses τ^{-1} to set the actual squares to the positions that σ can be applied, (2) applies σ and (3) applies τ to put them back.

Idea 3 (Set Them Up & Put Them Back)**.** *Suppose $\sigma \in \mathcal{P}$ permutes the squares $x_1, \ldots, x_m$ in a desirable way but σ cannot be applied to the squares $y_1, \ldots, y_m$. If there is a permutation $\tau \in \mathcal{P}$ such that $\tau(x_i) = y_i$, then $\tau\sigma\tau^{-1}$, the conjugate of σ by τ, permutes $y_1, \ldots, y_m$ in the same desirable way by Lemma 4 & 5.*

2.4 Commutators

Since a Rubik's Cube has many squares, the squares have to be solved in some ordering. When solving the remaining squares, we like to preserve the squares which already have been solved. The concept of commutators is very useful for achieving such goal. We discuss how to do it in the following sections.

2.4.1 Substitutions

Suppose we want to cycle the contents of 03, 15, 04. It is relatively easy to come up with a sequence of moves doing it while at the same time the moves have a side effect scrambling other squares. Let

$$V := [B^{-1}, R]^2 = (BR^{-1}B^{-1}R)^2 \quad \text{and} \quad V_1 := \big(03 \quad 15 \quad 04\big)\,.$$

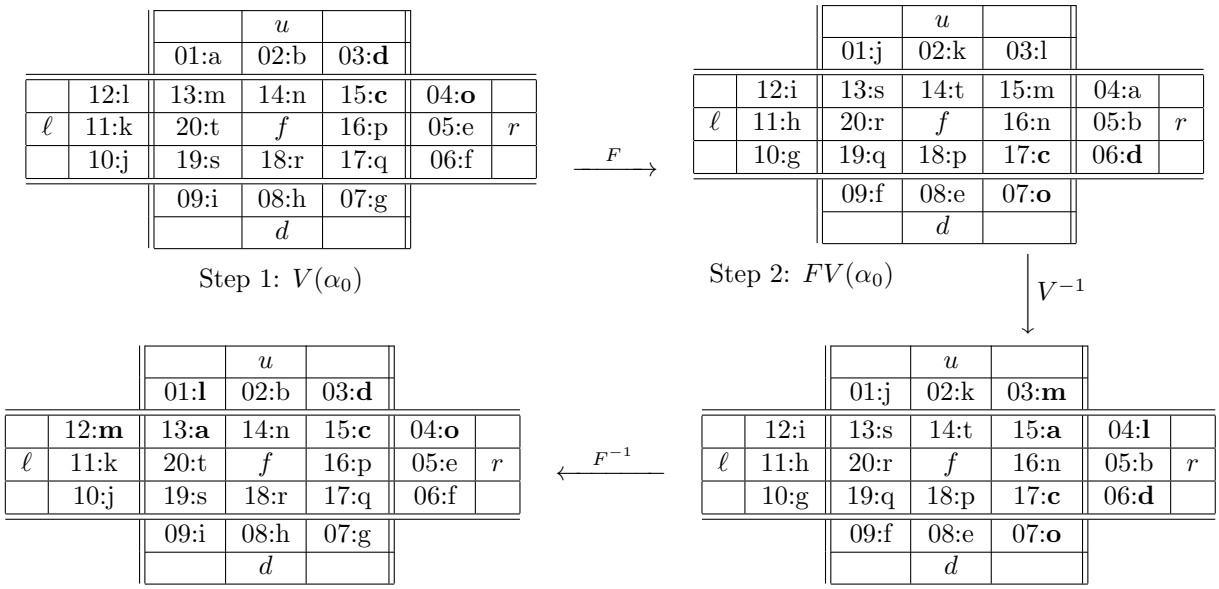
Similar to M^2 described in Section 2.2, V consists of six 3-cycles including V_1 while it preserves all the remaining squares ≤ 20 as shown in the Step 1 of Figure 2. Note that V also scrambles some of the squares > 20 which are not shown in the figure. How about V^{-1}? It reverts V – it has a cycle $V_1^{-1} = \big(03 \quad 04 \quad 15\big)$, preserves all the remaining squares ≤ 20 and moves back the squares > 20 which V has scrambled. If V^{-1} is applied right after V, it has no effect by definition. However, we may

1. apply V to cycle the letters in 03, 15, 04 with a side effect scrambling some of the squares > 20;
2. substitute the letters in 03, 15, 04 with some of the letters preserved by V;
3. apply V^{-1}, which cycles inversely the substituted letters and reverts the side effect; and
4. undo the substitution.

The original 3 letters are cycled in one direction and the substituted 3 letters are cycled in the reversing direction. How to do the substitution? By design, V cycles 03, 15, 04 and preserves all the remaining ≤ 20 squares. A substitution can be done simply by F. The 4-step permutation actually is the commutator

$$[F, V] \quad := \quad F^{-1}V^{-1}FV \quad = \quad \big(03 \quad 15 \quad 04\big)\big(01 \quad 13 \quad 12\big)\,.$$

Amazingly, the six 3-cycles in V is reduced to only two in $[F, V]$. It moves fewer squares (Idea 0).



Step 1: $V(\alpha_0)$ Step 2: $FV(\alpha_0)$ Step 3: $V^{-1}FV(\alpha_0)$ Step 4: $F^{-1}V^{-1}FV(\alpha_0)$

Figure 2: A 4-Step Substitution

Idea 4 (Think Substitution)**.** *For permuting the contents of some targeted squares in a desirable way,*

1. *find $\sigma \in \mathcal{P}$ to permute them, where σ may have a side effect scrambling some other squares;*
2. *apply a substitution $\tau \in \mathcal{P}$;*
3. *apply σ^{-1}, which permutes inversely the substituted contents and reverts the side effect; and*
4. *apply τ^{-1} to undo the subsitution.*

2.4.2 A 3-Cycle as Two Transpositions

Idea 4 can as well be used to construct permutations consisting of 3-cycles using equation (1). Let $\mathcal{A} := \{a_1, \cdots, a_m\}$, $\mathcal{B} := \{b_1, \cdots, b_m\}$ and $\mathcal{C} := \{c_1, \cdots, c_m\}$ be disjoint sets with the same size m. Then,

1. swap the contents of b_i's and c_i's while it may have a side effect scrambling some other squares;
2. substitute the contents of b_i's and c_i's respectively with a_i's and b_i's;
3. undo the swap, which swaps the substituted contents and reverts the side effect; and
4. undo the substitution.

Such 4-step permutation is decomposed into 3-cycles $(a_1 \quad b_1 \quad c_1) \cdots (a_m \quad b_m \quad c_m)$.

Idea 5 (3-Cycle)**.** *Use pairs of transpositions to construct 3-cycles as described in Lemma 2.*

Example 3. Let $\mathcal{A} := \{09, 19, 10\}$, $\mathcal{B} := \{01, 12, 13\}$ and $\mathcal{C} := \{15, 04, 03\}$. Recall in equation (3) that T consists of 6 transpositions. Indeed, for some $a, b, c > 20$,

$$T \quad = \quad (01 \quad 15)\,(12 \quad 04)\,(13 \quad 03)\,(06 \quad a)\,(07 \quad b)\,(17 \quad c)\,.$$

The first 3 cycles are exactly the transpositions for swapping b_i's and c_i's while the last 3 cycles are unwanted. Idea 3 can be used to relocate the unwanted cycles. Let $W := DTD^{-1}$ be the conjugate of T by D, where D^{-1} temporarily moves away the contents of 06, 07, 17 to some squares > 20 and D moves them back at the end. Now, apply Idea 4 with W as the permutation (σ) and F as the substitution (τ). Since $T^{-1} = T$, we have $W^{-1} = DT^{-1}D^{-1} = W$ by Lemma 1. The final permutation is the commutator

$$[F, W] \quad := \quad F^{-1}WFW \quad = \quad (01 \quad 15 \quad 09)\,(12 \quad 04 \quad 19)\,(13 \quad 03 \quad 10)\,, \tag{4}$$

which consists of three disjoint 3-cycles. The 4 steps are shown in Figure 3 below.

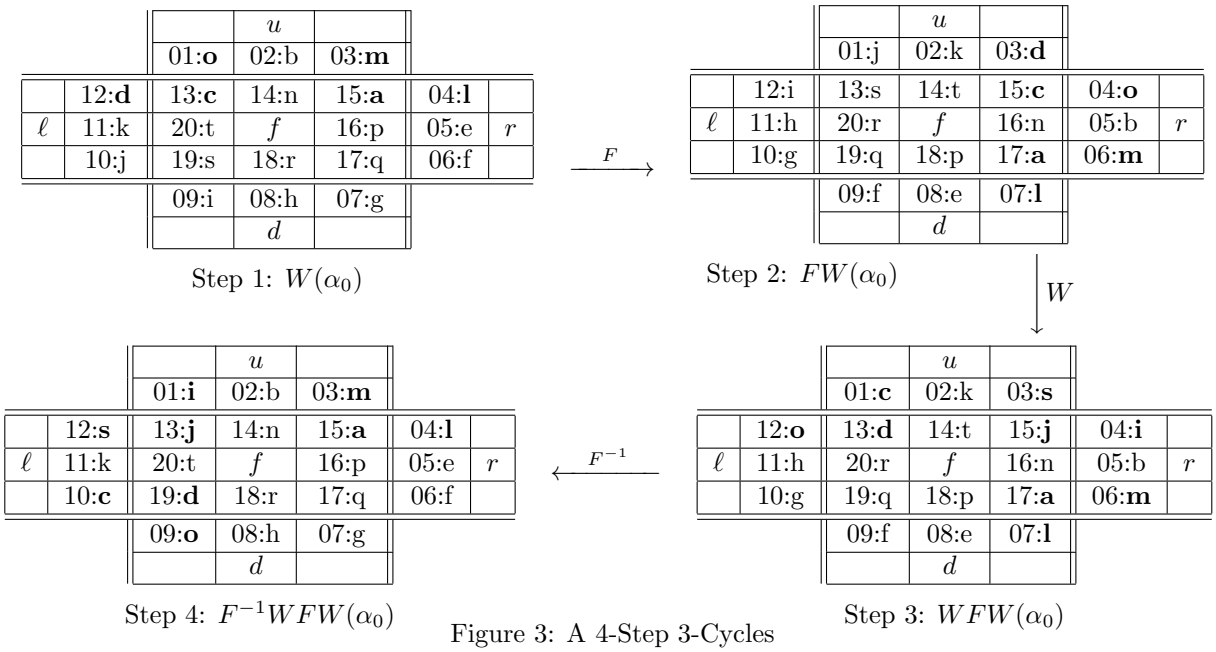


Figure 3: A 4-Step 3-Cycles

How to construct a permutation of 3-cycles with $\mathcal{B}, \mathcal{C}, \mathcal{D}$ instead of $\mathcal{A}, \mathcal{B}, \mathcal{C}$, where $\mathcal{D} := \{06, 07, 17\}$? We may either (i) replace the substitution F with F^{-1} in equation (4), i.e. the final permutation becomes $[F^{-1}, W]$ instead of $[F, W]$; or (ii) conjugate $[F, W]$ by $\tau := F$ or $\tau := D$ using Idea 3. Approach (ii) is more flexible than Approach (i) in the sense that the new substitution in Approach (i) must preserve all the squares > 20 while the permutation τ in Approach (ii) may scramble them. Also, Approach (i) may not work if $\mathcal{D}$ has squares > 20. Note that the resulted permutations from these approaches can be different – they all consist of 3-cycles but the 3-cycles can be different.

3 A Final Note

Once again, solving Rubik's cube is not easy. In the beginning, it is even difficult to remember the moves and the positions of the squares. It may be helpful to write them down and perform the moves slowly.

Enjoy Rubik cubing and add oil !