Structure and generation properties of the Rubik's cube group

Ravi Fernando

University of California, Berkeley *fernando@berkeley.edu*

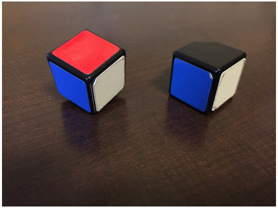
August 4, 2017

Anatomy of a Rubik's cube

A disassembled Rubik's cube contains:

- 1 core with 6 stationary face centers
- 8 corner pieces with 3 stickers each
- 12 edge pieces with 2 stickers each

Since the center pieces never move relative to each other, we use them as reference points to determine where all the other pieces should be placed.



The cheater's Rubik's cube group

We define the "cheater's Rubik's cube group" $\overline{G}$ to be the set of all operations that can be done to a Rubik's cube by taking it apart and putting it back together. This allows us to do four things:

- Permute the 12 edge pieces
- Flip any subset of the edges in place
- Permute the 8 corner pieces
- Twist any subset of the corners in place

This gives us the group

$$\overline{G} = (\mathbb{Z}_2^{12} \rtimes S_{12}) \times (\mathbb{Z}_3^8 \rtimes S_8) \quad (1)$$

$$= (\mathbb{Z}_2 \wr S_{12}) \times (\mathbb{Z}_3 \wr S_8), \quad (2)$$

with order $|\overline{G}| = 2^{12} \cdot 12! \cdot 3^8 \cdot 8! \approx 5 \cdot 10^{20}$.

The actual Rubik's cube group

The Rubik's cube group G is defined to be the subgroup of $\overline{G}$ generated by the 90-degree clockwise rotations of the six faces, which we denote U, F, R, B, L, and D. This fails to be the full group $\overline{G}$ because of three parity-like restrictions that are necessary for a given Rubik's cube configuration to be solvable:

- (index 2) the total number of edges flipped must be even.
- (index 3) the total number of clockwise corner rotations must be a multiple of 3.
- (index 2) the overall permutation of corners and edges must be an even permutation.

In fact, G is a normal subgroup of $\overline{G}$ with index $2 \cdot 3 \cdot 2 = 12$, so it has order

$$|G| = \frac{2^{12} \cdot 12! \cdot 3^8 \cdot 8!}{12} = 43,252,003,274,489,856,000. \qquad (3)$$

Another description

An equivalent description of G is as the semidirect product $G_O \rtimes G_P$, where G_O describes all orientations (flips and twists) of pieces, and G_P describes all permutations. These groups have the following structure:

- $G_O \cong \mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$, which we view as the subgroup of $\mathbb{Z}_2^{12} \times \mathbb{Z}_3^8$ where the $\mathbb{Z}_2$-coordinates sum to $0 \pmod 2$, and the $\mathbb{Z}_3$-coordinates sum to $0 \pmod 3$. Each coordinate represents the flipping of an edge or the twisting of a corner.
- $G_P = (S_{12} \times S_8) \cap A_{20}$, where we view $S_{12} \times S_8$ as a subgroup of S_{20} in the obvious way. That is, we can do any permutation of the 12 edges and any permutation of the 8 corners, as long as the two permutations have the same parity.

To construct the semidirect product, we let G_P act on G_O by permuting the coordinates.

Generating sets

The most obvious generating set of G, $\{U, F, R, B, L, D\}$, is redundant: any one of the six generators can be expressed in terms of the others. However, any five out of six form an irredundant generating set.

Question

Can we generate G with fewer elements, or with more irredundant elements?

- $r(G)$ = minimal number of generators = 2.
- $m(G)$ = maximal number of irredundant generators = ?.
- $i(G)$ = maximal number of irredundant elements = ?.

Two lemmas for calculating m

Our goal is to calculate $m(G)$. We will use two related lemmas:

Lemma 1

If G is any group and N is a normal subgroup, then $m(G) \leq i(N) + m(G/N)$.

Lemma 2

If N is a minimal normal subgroup of G and N is abelian, then

$$m(G) = \begin{cases} m(G/N) & \text{if } N \text{ is contained in the Frattini subgroup } \Phi(G), \\ 1 + m(G/N) & \text{otherwise.} \end{cases} \tag{4}$$

(A *minimal normal subgroup* is a subgroup that is inclusion-minimal among nontrivial normal subgroups.)

Finding abelian minimal normal subgroups

Since $G_O \cong \mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$ is an abelian normal subgroup of G, we look inside it for abelian minimal normal subgroups. We have a chain of normal subgroups of G:

$$1 < Z < G_{EO} < G_O < G, \tag{5}$$

where:

- $Z \cong \mathbb{Z}_2$ is the center of G, generated by the "superflip",
- $G_{EO} \cong \mathbb{Z}_2^{11}$ is the edge orientation group, which contains edge flips but not corner twists, and
- $G_O \cong \mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$ is the full orientation group as before, including edge flips and corner twists.

Applying lemma 2

Given the chain

$$1 < Z < G_{EO} < G_O < G, \tag{6}$$

we now apply lemma 2 three times, with three successive choices of abelian minimal normal subgroups:

- The center Z of G equals the Frattini subgroup, so $m(G) = m(G/Z)$.
- G_{EO}/Z is minimal normal in G/Z. It is abelian and not contained in the Frattini subgroup, so the quotient $(G/Z)/(G_{EO}/Z) = G/G_{EO}$ satisfies $m(G) = 1 + m(G/G_{EO})$.
- G_O/G_{EO} is minimal normal in G/G_{EO}. It is abelian and not contained in the Frattini subgroup, so the quotient $(G/G_{EO})/(G_O/G_{EO}) = G/G_O$ has $m(G/G_{EO}) = 1 + m(G/G_O)$.

So $m(G) = 2 + m(G/G_O) = 2 + m(G_P)$.

Calculating $m(G_P)$: upper bound

We now only need to calculate m of $G_P = (S_{12} \times S_8) \cap A_{20}$. We can't apply lemma 2 anymore, because there are no more abelian minimal normal subgroups. Instead, we apply lemma 1.

Observe that G_P contains the normal subgroup $N = A_{12} \times 1$, with $G_P/N \cong S_8$. So lemma 1 gives:

$$\begin{aligned} m(G_P) &\leq i(A_{12}) + m(S_8) && (7) \\ &= (12 - 2) + (8 - 1) = 17. && (8) \end{aligned}$$

Here we use Whiston's theorem that S_n has $m = i = n - 1$ and A_n has $m = i = n - 2$.

Calculating $m(G_P)$: lower bound

In order to show that $m(G_P)$ is equal to 17, we exhibit an explicit irredundant generating set of this size. We choose:

- ten 3-cycles of edges: $(1, 2, 3), \dots, (1, 2, 12)$;
- six 3-cycles of corners: $(13, 14, 15), \dots, (13, 14, 20)$; and
- one double transposition: $(1, 2)(13, 14)$.

The subgroup generated by all but the last of these elements is $A_{12} \times A_8$, and adding the last generates the full G_P. But if we remove (e.g.) the 3-cycle $(1, 2, 3)$, then all of the remaining elements fix the point 3. So this is an irredundant generating sequence of G_P, and therefore $m(G_P) \geq 17$.

Conclusion

Since we calculated that $m(G_P) = 17$, it follows that

$$m(G) = 2 + 17 = 19. \tag{9}$$

So among any set of elements generating G, some subset of size at most 19 suffices to generate.

References

Image sources:

- http://cubercritic.com/wp-content/uploads/2013/05/3x3-Core.jpg
- https://jb3designs.files.wordpress.com/2015/01/126.jpg