Algebra 1 Honours, ASE Rubik's Cube

We always compose and apply functions from left to right (opposite of the usual convention).

Lecture 1

We first give a careful definition of the Rubik's group.

Definition 1. The cube is made up of 27 small cubes called *cubies* (there are three layers of nine cubies; one cubie is not visible, and in fact does not really exist). Each cubie has one, two or three visible faces, called facelets. If a cubie has one facelet it is a *center cubie*, two facelets an *edge cubie*, and otherwise is a *corner cubie.* The positions occupied by cubies are called *cubicles* and the positions occupied by faclets are called *slots.* A *state of the cube* is a bijection $\{\text{facelets}\} \xrightarrow{\cong} \{\text{slots}\}$. Note there are 54! states. We set $\mathcal{S}$ to be the set of states of the cube.

Label the center cubies by F, B, U, D, L, R and the corresponding center cubicles by f, b, u, d, l, r (to label, we can pick F arbitrarily, and then choose U to be an arbitrary adjacent slot; the others are then determined). We view moves of the cube as elements of $\mathrm{Perm}(\mathcal{S})$, and let $F, B, U, D, L, R \in \mathrm{Perm}(\mathcal{S})$ be rotation by 90° clockwise around the given face (if one is viewing the face). The *Rubik's group* G is the subgroup of $\mathrm{Perm}(\mathcal{S})$ they generate:

$$G = \langle F, B, U, D, L, R \rangle \subseteq \mathrm{Perm}(\mathcal{S}).$$

We call elements of the Rubik's group *moves.* If $\sigma \in \mathcal{S}$ is a state and $g \in G$ is a move, *the action of g on σ*, written σg, is the value of the permutation g on σ. We denote the *start state* (i.e., the state the cube arrives in) by e. The set $\mathcal{P}$ of *possible states* is

$$\mathcal{P} = \{eg \mid g \in G\}.$$

Solving the cube amounts to, given $\sigma \in \mathcal{P}$, find $g \in G$ such that $\sigma g = e$.

Definition 2. We will label cubicles by the faces their facelets are on, e.g., ur is the edge cubicle with one facelet on U and one facelet on R; the cubicle urf is the corner cubicle with one facelet on U, one facelet on R, and one facelet on F. *We always label corner cubicles by listing the faclets in clockwise order, looking from the corner to the middle of the cube.* So every corner can be written exactly three ways, e.g., $urf = rfu = fur$, but not ruf.

We can write elements of G using cycle notation, for instance,

$$R = (urf, bru, drb, frd)(ur, br, dr, fr).$$

This is telling us how R acts on any given state: the facelet in the u slot of the ufr cubicle is sent to the b slot of the bur cubicle, etc. In fact, when we write a cycle representing $g \in G$, we are writing a bijection $\psi : \{\text{slots}\} \to \{\text{slots}\}$ such that $\sigma g = \sigma \circ \psi = \{\text{facelets}\} \xrightarrow{\sigma} \{\text{slots}\} \xrightarrow{\psi} \{\text{slots}\}$, for all states $\sigma \in \mathcal{S}$.

Example 3. To find the cycle notation of a move, pick a corner cubie and record the positions of its facelets under iterations of the move, until the cubie reaches the position it started in. Then pick a corner cubie that did not arise in the previous cycle, and repeat. Do this until all the corner cubies have been accounted for (if a cubie doesn't move, don't write anything). Repeat this for edges, e.g.,

$$RU = (urf, rfu, fur)(ufl, ulb, ubr, bdr, dfr, luf, bul, rub, rbd, rdf, flu, lbu, bru, drb, frd)(fr, uf, ul, ub, ur, br, dr).$$

This example shows that the order we write the adjacent facelets of a cubicle is important: (urf, rfu, fur) is not (urf, urf, urf) because the later is the identity, but RU does move the facelets currently in the urf cubicle: it rotates them counterclockwise. Similarly, $(RU)^5$

rotates the facelets in the ubr cubicle counterclockwise. We can shorten cycle notation by incorporating these twists, e.g.,

$$\begin{aligned} RU &= (urf)_+(ufl, ulb, ubr, bdr, dfr)_-(fr, uf, ul, ub, ur, br, dr) \\ URU^{-1}R^{-1} &= (ulb, ubr)_+(dfr, rfu)_-(ur, fr, ub). \end{aligned}$$

Here the $+$ means clockwise, and $-$ means counterclockwise. We can do the same for edges, e.g.,

$$FRUR^{-1}U^{-1}F^{-1}U = (uf)_+(ul, bu)_+(ufl)_+(ulb, fur)_-.$$

Example 4. Finding cycle notation is a bit tedious. We can use relabeling of the faces to help. For instance, we found the cycle decomposition of $[U, R] = URU^{-1}R^{-1}$ above; can we relabel to find the cycle decomposition of $[U, L] = ULU^{-1}L^{-1}$? First, we consider the bijection of faces $\widetilde{\phi} : \{f, b, u, d, l, r\} \to \{f, b, u, d, l, r\}$ with $\widetilde{\phi}(l) = r, \widetilde{\phi}(r) = l, \widetilde{\phi}(f) = b, \widetilde{\phi}(b) = f, \widetilde{\phi}(u) = u, \widetilde{\phi}(d) = d$ (we can write this in cycle notation for permutations as $\widetilde{\phi} = (l, r)(f, b)$). We can extend this to a bijection $\phi : \{\text{slots}\} \to \{\text{slots}\}$ so e.g., the r slot of the urf cubicle to the $l = \phi(r)$ slot of the $ulb = \phi(u)\phi(r)\phi(f)$ cubicle. If ϕ is any such bijection, define $\phi' = e\phi e^{-1} : \{\text{facelets}\} \to \{\text{facelets}\}$ (recall $e : \{\text{facelets}\} \to \{\text{slots}\}$ is the start state) and set $C_\phi \in \mathrm{Perm}(\mathcal{S})$ to be the permutation that sends $\sigma \in \mathcal{S}$ to $\widetilde{\phi}^{-1}\sigma\phi$. The permutation C_ϕ relabels a given state: indeed, if σ is a state that takes a facelet X to some slot a, then σC_ϕ takes $(X)\phi'$ to $(a)\phi$, exactly as one would expect.

We now consider another bijection $\psi : \{\text{slots}\} \to \{\text{slots}\}$, and let $R_\psi \in \mathrm{Perm}(\mathcal{S})$ be defined by $(\sigma)R_\psi = \sigma \circ \psi$. If ψ is in cycle notation describing a group element g, as described in Defintion 2, then $g = R_\psi$. I claim that relabeling by ϕ, doing the move g, then reverting to the original labeling is given by $C_\phi R_\psi C_{\phi^{-1}}$ (remember we compose from left to right). It follows from the definitions that $C_\phi R_\psi C_{\phi^{-1}} = R_{\phi\psi\phi^{-1}}$, thus $\phi\psi\phi^{-1}$ is giving our new cycle. What does this mean? Let's look at a simple example. Let ψ be the bijection given by the following cycle:

$$R = (urf, bru, drb, frd)(ur, br, dr, fr),$$

and let ϕ be the relabeling described above. What is $\phi\psi\phi^{-1}$? e.g., on ulb it is:

$$ulb \xrightarrow{\phi} urf \xrightarrow{\psi} bru \xrightarrow{\phi^{-1}} flu.$$

Another way to say this is, it maps $\phi^{-1}(urf) \mapsto \phi^{-1}(bru)$. Thus, to find the cycle notation for $\phi\psi\phi^{-1}$, we apply ϕ^{-1} to every face that appears. If we do this to the cycle notation for R we get

$$(ulb, flu, dlf, bld)(ul, bl, dl, fl)$$

which is the cycle notation for L, exactly as we would hope. Applying ϕ^{-1} to the cycle notation for $[U, R]$ gives

$$[U, L] = (urf, ufl)_+(dbl, lbu)_-(ul, bl, uf).$$

Let's check one more. What is $[U, F]$? Here we use the relabeling given by $\phi = (f, l, b, r)$. Applying $\phi^{-1} = (f, r, b, l)$ to the cycle notation of $[U, L]$ gives:

$$[U, F] = (ubr, urf)_+(dlf, flu)_-(uf, lf, ur).$$

Questions to try: (you don't have to hand any of these in, but some may be on the homework assigned next week)

(1) Write the cycle decomposition of F^2R^2.
(2) Try (really hard) to solve the corners of your cube.
(3) Using the example above, $(URU^{-1}R)^3 = (ulb, bru)(urf, dfr)$. Does this help you solve the corners? Can you use this to find a move that involves the four upper corners? The four left corners? Two left corners and two right corners?

(4) Try writing down some cycle decompositions of random simple moves and repeating the above to find interesting cycle decompositions. For instance, can you find a move that cycles three corners and leaves everything else fixed? How would this help you solve the corners?

(5) Define the $2 \times 2 \times 2$ Rubik's group G_2 and show that there is a surjective group homomorphism $G \to G_2$. What is the kernel? Can you find specific moves that are in the kernel?

Lecture 2

We first show the following. It is meant to be motivation for the more precise description of possible moves we will prove next.

Proposition 5. *Any non-starting state of the cube $\sigma : \{facelets\} \to \{slots\}$ that sends all but two facelets to their starting slots is not a possible state.*

Recall a possible state was one of the form eg, where e is the start state and g is any element of G. Thus the proposition tells us there is no move that transposes two faclets and fixes the rest.

Proof. First recall that every element of a permutation group S_n can be written as a product of transpositions, and the parity of the number of transpositions is called the sign of a transposition (there are usually many ways to write any given element as a product of transpositions; the sign does not depend on which one we choose). If the sign is 0 we say the element is even, and if it's 1, the element is odd.

To apply this to the Rubik's group, we identify the states of the cube $\mathcal{S}$ with the permutation group S_{54} as follows. Pick a bijection $\alpha : \{\text{facelets}\} \xrightarrow{\cong} \{1, \ldots, 54\}$, and set $e^{-1}\beta : \{\text{slots}\} \xrightarrow{\cong} \{1, \ldots, 54\}$ (these are just labelings of the facelets and the slots, such that the labelings coincide when a facelet is in its starting slot). Now given a state $\sigma : \{\text{facelets}\} \xrightarrow{\cong} \{\text{slots}\}$, we can consider the bijection $\beta\sigma\alpha^{-1} : \{1, \ldots, 54\} \xrightarrow{\cong} \{1, \ldots, 54\} \in S_{54}$. Conversely, given any $\phi \in S_{54}$, consider the state $\beta^{-1}\phi\alpha : \{\text{facelets}\} \xrightarrow{\cong} \{\text{slots}\}$. These assignments are a bijection $\mathcal{S} \xrightarrow{\cong} S_{54}$. If $e \in \mathcal{S}$ is the start state, there is an injection

$$\begin{aligned} G &\to \mathcal{S} \\ g &\mapsto e \cdot g, \end{aligned}$$

whose image is the possible states. So combined with the above, we can view G as a subset of S_{54}, i.e., view each element of G as a permutation of the facelets, and then we can ask what the sign of that element of G is. We first find the sign of U. Label the facelets on the outside upper layer $1, \ldots, 12$, in a clockwise way, and label the non-center facelets on the up face $13, \ldots, 20$, again in a clockwise way. Then

$$U = (1, 4, 7, 10)(2, 5, 8, 10)(3, 6, 9, 12)(13, 15, 17, 19)(14, 16, 18, 20)$$

and this is an even element (each 4 cycle is odd, and there are 5). We can apply an isomorphism to take U to any face, and an isomorphism preserves sign, so D, L, R, F, B are also all even. Since the product of even elements is even, and the inverse of an even element is even, every element of G is even, since it is generated by U, D, L, R, F, B. □

To describe the possible states more precisely, we put a mark on one slot of each cubicle and one facelet of each cubie, in such a way that the marks coincide when a cubie is in its start cubicle.

Definition 6. The *marked slot of a cubicle* is the u or d slot, if the cubicle is in the up or down layer, and is the l or r slot otherwise. The *marked facelet of a cubie* is the facelet that is in the marked slot when the cubie is in start position.

In a given state, the *twist* of a corner cubie is 0 if the marked facelet is in the marked slot, 1 if the marked facelet is 120° clockwise from the marked slot, and 2 otherwise. Analogously, the *flip* of an edge cubie is 0 if the marked facelet is in the marked slot and 1 otherwise.

Given a state of the cube, convince yourself that the cubicle and twist or flip of a cubie determines the slots of all of its facelets. It follows that we can describe a move by permutations of cubies (as opposed to the facelets we were considering), and a twist or flip of each cubie. If we label the corner cubicles $1, \ldots, 8$, the edge cubicles $1, \ldots, 12$, and cubies by their start cubicles, then we can describe a state as a quadruple $(\rho, \sigma, \boldsymbol{x}, \boldsymbol{y})$, with $\rho \in S_8, \sigma \in S_{12}, \boldsymbol{x} = (x_1, \ldots, x_8), \boldsymbol{y} = (y_1, \ldots, y_{12})$ and $x_i \in \{0,1,2\}, y_i \in \{0,1\}$.[1] The corresponding state will send the ith corner cubie to the $\rho(i)$th corner cubicle with twist x_i, and the jth edge cubie to the $\sigma(j)$th edge cubicle with flip y_j.

Note that since the center cubies are in their start cubicles in every possible state, every possible state can be described by a quadruple, as above. The following characterizes the quadruples that are possible states.

Theorem 7 ("Main Theorem of Cubology")**.** *A quadruple $(\rho, \sigma, \boldsymbol{x}, \boldsymbol{y})$, with $\rho \in S_8, \sigma \in S_{12}, \boldsymbol{x} = (x_1, \ldots, x_8), \boldsymbol{y} = (y_1, \ldots, y_{12})$ and $x_i \in \{0,1,2\}, y_i \in \{0,1\}$ represents a possible state if and only if the following three conditions hold:*

(1) $\operatorname{sgn} \rho = \operatorname{sgn} \sigma$,
(2) $x_1 + \ldots + x_8 = 0$ *mod 3,*
(3) $y_1 + \ldots + y_{12} = 0$ *mod 2.*

This is a very powerful theorem. It was first proved by Anne Scott, and publicized in the book "Winning Ways for Your Mathematical Plays, Vol. 4" by Berlekamp, Conway, and Guy. We will prove it next week in class. The proof of necessity (showing that a possible position satisfies the three conditions) is relatively easy; the proof of sufficiency (showing that if a quadruple satisfies these three conditions, then it is possible) is harder.

Using the bijection of G with the set of possible states, given by sending $g \in G$ to eg, where e is the start state, we can also apply the theorem to the Rubik's group. For instance, this immediately shows that there is no element of the group that twists two corners in the same direction and leaves every other facelet fixed, but there are moves that twist three corners in the same direction and leave every other facelet fixed. You will see other applications of the theorem in the exercises.

Lecture 3 Summary

We will start writing $'$ for inverses, so e.g., $L' = L^{-1}$.

- We used Z-commutators, see appendix, to find a corner 3-cycle. We came up with

$$L'B'[U,R]^3 BL[U,R]^3 = (ulb, luf, bru).$$

  We'll find a shorter, better corner 3-cycle later, but the idea here was to take the cycle decomposition of $[U,R]$, and simple conjugation, to come up with this.
- We talked more about the flip and twist of a cubie, and did some examples.
- We talked more about how quadruples describe states.
- We then used F^2R^2 and related moves to find an edge 3-cycle. We came up with

$$(D'F^2)'[(F^2R^2)^3, F](D'F^2) = (ur, uf, ul).$$

  Again, we will find a shorter move to do this later, but the point was to take F^2R^2 and work from there.
- Finally, we started the proof of the main theorem.

[1] We can't describe every state with such a quadruple, just the ones that we can reach by taking apart the cube and reassembling it, i.e., the states with the center cubies in their start position, and the facelets on each cubie in their original position on that cubie.

Lecture 4 Summary

- We talked about conjugation, e.g., $F[U, R]F'$.
- Discussed normal subgroups of the cube, and how the usefulness of conjugation shows most subgroups of the cube group are not normal. We went over the example $\langle U, R\rangle$ in detail, showing it is not normal.
- We finished the proof of the main theorem.
- Talked about corollaries, including the order of the group, and how corners can be moved (mesons and baryons).

Proof of the Main Theorem

(coming soon)
We will use the following moves...edge 3-cycle, corner 3-cycle, monoflip, monotwist,....

Lecture 5 Summary

We talked briefly about how the Rubik's group G acts on the set of states $\mathcal{S}$. We spent the rest of the hour going through the step by step solution below.

Solution of the cube

There is a cheat sheet with diagrams on the next page.

(1) Solve the bottom layer.
(2) Solve the middle layer. Use the commutator $[U, R][F, R'] = (uf, rf, bu)(ulb, rub, rfu)$ to move uf to rf or the commutator $[U', L'][F', L] = (uf, lf, bu)(ulb, rub, rfu)$ to move uf to lf. (Note these moves only effect the rf or lf cubie in the middle layer, and otherwise leave the bottom two layers untouched.) If you need to move a cubie within the middle layer, first move it to the upper layer using one of the above, and then use the appropriate one to move it back down in the correct position.
(3) Flip upper layer edges so correct color is on up face. Use $F[U, R]F' = (ur, fu, ub)(ufl, urf)_-(ulb, ubr)_+$ or its inverse $F[R, U]F'$.
(4) Permute the upper layer edges to their start cubicles. Use $(FU)[U, F'](FU)' = (ur, uf, ub)(ulb, fur)_-(ufl, rub)_+$, or its inverse $(FU)[F', U](FU)'$, or the edge 2-cycle $(FU)[U, F'](FU)'U' = (ul, uf)(ufl, bul, urf)$.
(5) Permute the upper layer corners to their start cubicles. Use $[L', URU'] = (ulb, rub, flu)$ or its inverse $[URU', L']$.
(6) Untwist the upper corners. Orient the cube so that a twisted corner is in the urf cubicle. Apply $[R', D']$ repeatedly until that corner is untwisted in the urf cubicle. Then rotate the upper layer so that anther untwisted corner is in urf. Again, apply $[R', D']$. Repeat this until all upper corners are untwisted. You will end with a solved cube.

Proof. It is clear that $[R', D']^2$ will twist the cubie in urf by 1, and leave the rest of the upper layer fixed. Thus we can assume that we have untwisted three upper corner cubies, and are left with one corner untwisted (the bottom two layers will not necessarily be in their start states). Because the drf cubie is in its start position, we must have done an even number of iterations of $[R', D']$ to get to this point. Say we have done $2n$ iterations. Label the corner cubies so $1 = urf, 2 = drf, 3 = drb, 4 = dlb$, and the rest arbitrarily. Let x_i be the twist of the ith corner cubie, and assume that $x_1 = k$. Since we have done $2n$ iterations of $[R', D']$ we must have $x_2 = n, x_3 = 2n, x_4 = 2n$. By the Main Theorem we must have

$$k + 5n = 0 \,(\mathrm{mod}\, 3) \quad \text{i.e.,} \quad k = n \,(\mathrm{mod}\, 3).$$

If $k = 0$, then $n = 0$ mod 3, so $2n = 0$ mod 6. Since $[R', D']$ has order 6, and we have done $2n$ iterations of it, the cube is in its start state. If $k = 1$, then $2n = 2$ mod 6. Doing four more iterations of $[R', D']$ will untwist corner cubie 1, and will bring the total iterations of $[R', D']$ to $2n + 4 = 0 \bmod 6$, and so the cube is solved. Finally, if $k = 2$, then two iterations of $[R', D']$ will untwist corner cubie 1 and we will have done $2n + 2$ iterations of $[R', U']$, and $2n + 2 = 0 \bmod 6$, so the cube is solved. □

Moves used in solution

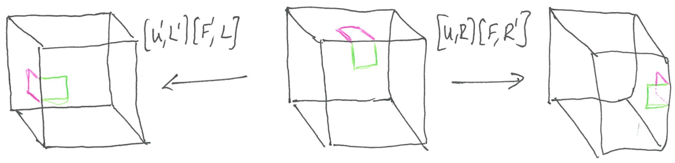
All of the moves listed are the *clockwise versions.* The counterclockwise versions are the inverses of the moves below. It is very helpful to note that for any group G, with elements $g, x \in G$, we have

$$(gxg^{-1})^{-1} = gx^{-1}g^{-1} \text{ and } [g, x]^{-1} = [x, g].$$

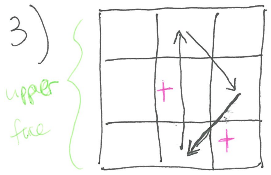
So, for example, $[L', URU']^{-1} = [URU', L']$ will give a counterclockwise 3 cycle of corners.

1) by hand

2)

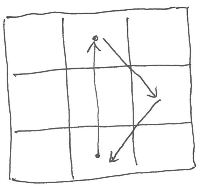


3)

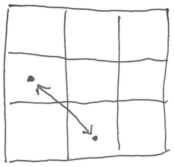


$F[R,U]F'$

4)

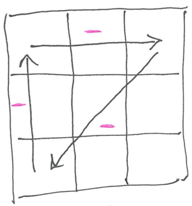


$FU[U,F'](FU)'$



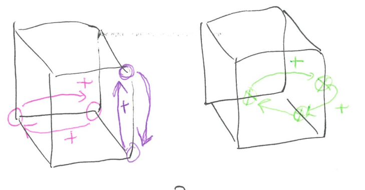
$FU[U,F'](FU)'U'$

5)



$[L', URU']$

6)



$[R', D']$

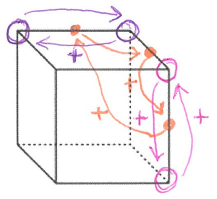
Appendix

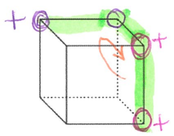
Monoflip: $T = FUD'L^2U^2D^2RU$. This flips the uf edge and fixes everything else in the upper layer, so e.g., $[T, U] = (uf)_+(ur)_+$.

Monotwist: $W = R'DRFDF'$. This twists the urf corner by 1 and fixes everything else in the the upper layer, so e.g., $[W, U] = (urf)_+(ubr)_-$.

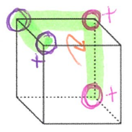
Z-Commutators

$[U, R] = (ulb, ubr)_+(dfr, rfu)_-(ur, fr, ub)$

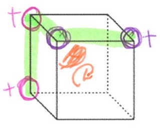




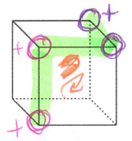
$[U, R]$



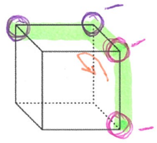
$[U, B]$



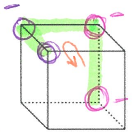
$[U, L]$



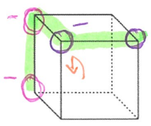
$[U, F]$



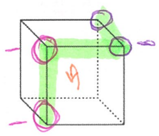
$[R, U]$



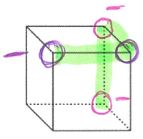
$[B, U]$



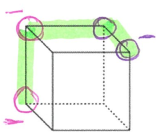
$[L, U]$



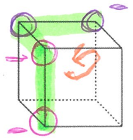
$[F, U]$



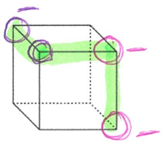
$[U', R']$



$[U', B']$



$[U', L']$



$[U', F']$