THE 15-PUZZLE (AND RUBIK'S CUBE)

KEITH CONRAD

1. Introduction

A permutation puzzle is a toy where the pieces can be moved around and the goal is to reassemble the pieces into their beginning state. We will discuss two such puzzles: the 15-puzzle and Rubik's Cube. Our analysis of the 15-puzzle will be complete, but we will only sketch some basic ideas behind the mathematics of Rubik's Cube.

2. The 15-puzzle

The 15-puzzle contains 15 sliding pieces and one empty space. It looks like this:

(2.1)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

After moving the pieces around until they are jumbled pretty thoroughly, the task is to bring the pieces back to the arrangement above.

Today 15-puzzles are usually sold with the pieces in a single casing so they can't be removed, but the puzzle originally had *removable* pieces. Figure 1 shows a modern 15-puzzle where the pieces can be taken out (not easy to find!).

Figure 1. A 15-puzzle with removable parts where pieces 14 and 15 are swapped.

The original challenge of the puzzle (with removable pieces) was to start in the state (2.2), with 14 and 15 switched, and return to the numerically ordered state (2.1).

(2.2)

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

The 15-puzzle was created in the 1870s in New England and was slow to catch on at first, but in 1880 it swept very quickly across America and Europe. Many people came forward announcing they could go from (2.2) to (2.1), but either they were unable to demonstrate their winning sequence of moves in public or they misunderstood the challenge itself. Starting in the 1890s, Sam Loyd offered a \$1000 prize (worth over \$25000 today) for anyone who could show a solution, and it is commonly believed that Loyd invented the puzzle, but that is false.[1]

Since today's 15-puzzles usually can't have their pieces removed, we consider the original challenge of the puzzle in reverse order: can one start with (2.1) and obtain (2.2)? Loyd's prize was safe for him to offer because it is impossible to move the pieces between the configurations (2.1) and (2.2). To show this we will translate the task into a question about multiplying permutations in a symmetric group.

Our first task, which is adapted from [4, Sect. 5.1], is to explain how to *interpret* the puzzle's configurations (describe where each piece is located) and moves (describe how positions of pieces change) as permutations so that multiplying a move's permutation and a configuration's permutation gives us the new configuration after applying the move.

Each piece in the puzzle is numbered in a natural way from 1 to 15. To keep track of the empty space, call it piece 16. Each position in the puzzle also is numbered in a natural way from 1 to 16. The same set $\{1, \ldots, 16\}$ can keep track of puzzle pieces and puzzle positions.

Definition 2.1. If C is a configuration of the puzzle pieces, including the empty space, view C as a permutation in S_{16} by the rule $C(i) =$ position of piece i, for $1 \leq i \leq 16$.

If M is a move of the puzzle pieces, view M as a permutation in S_{16} by the rule $M(i) =$ position where M moves the piece in position i, for $1 \leq i \leq 16$.

Different pieces of the puzzle are in different positions and every position is filled by some piece, so $C\colon \{1, \ldots, 16\} \to \{1, \ldots, 16\}$ is a permutation. Similarly, a move sends pieces in different positions to different positions, and each position after a move is filled by a piece from somewhere, so the function $M\colon \{1, \ldots, 16\} \to \{1, \ldots, 16\}$ is a permutation.

Example 2.2. The configuration

8	12	2	5
11	1	6	
7	14	10	15
9	4	3	13

is described by the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 6 & 3 & 15 & 14 & 4 & 7 & 9 & 1 & 13 & 11 & 5 & 2 & 16 & 10 & 12 & 8 \end{pmatrix},$$

which has disjoint cycle decomposition[2] $(1\ 6\ 7\ 9\ 13\ 16\ 8)(2\ 3\ 15\ 12)(4\ 14\ 10\ 11\ 5)$.

Example 2.3. The standard configuration (2.1) is described by the identity permutation and the configuration (2.2) is described by the 2-cycle $(14\ 15)$. More generally, (ij) in S_{16} describes the configuration where piece i is in position j, piece j is in position i, and piece k is in position k for $k \neq i, j$.

[1] See [5] for more history on this puzzle.

[2] We multiply permutations from *right to left*, so $(12)(13) = (132)$. Some references on group theory and permutation puzzles, such as [3] and [4], instead multiply from left to right, saying $(12)(13) = (123)$.

Example 2.4. The puzzle moves

$$\begin{array}{|c|c|c|c|}\hline 8 & 12 & 2 & 5 \\ \hline 11 & 1 & 6 & \\ \hline 7 & 14 & 10 & 15 \\ \hline 9 & 4 & 3 & 13 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|c|c|}\hline 8 & 12 & 5 & 6 \\ \hline 11 & 1 & 2 & \\ \hline 7 & 14 & 10 & 15 \\ \hline 9 & 4 & 3 & 13 \\ \hline \end{array} \tag{2.3}$$

and

$$\begin{array}{|c|c|c|c|}\hline 6 & 4 & 1 & 9 \\ \hline 10 & 12 & 8 & \\ \hline 2 & 13 & 7 & 5 \\ \hline 14 & 3 & 15 & 11 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|c|c|}\hline 6 & 4 & 9 & 8 \\ \hline 10 & 12 & 1 & \\ \hline 2 & 13 & 7 & 5 \\ \hline 14 & 3 & 15 & 11 \\ \hline \end{array}$$

are the same physical move M applied to different configurations. Obviously M is not done in one step! Each move arises from the following *basic* (one-step) moves in the upper right.

$$\begin{array}{|c|c|}\hline 2 & 5 \\ \hline 6 & \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 2 & 5 \\ \hline & 6 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline & 5 \\ \hline 2 & 6 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 5 & \\ \hline 2 & 6 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 5 & 6 \\ \hline 2 & \\ \hline \end{array} \tag{2.4}$$

$$\begin{array}{|c|c|}\hline 1 & 9 \\ \hline 8 & \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 1 & 9 \\ \hline & 8 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline & 9 \\ \hline 1 & 8 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 9 & \\ \hline 1 & 8 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 9 & 8 \\ \hline 1 & \\ \hline \end{array}$$

In terms of how M changes positions of pieces, what is in position 3 gets moved to position 7, what is in position 7 gets moved to position 4, what is in position 4 gets moved to position 3, and everything else stays put, so M as a permutation has $M(3) = 7$, $M(7) = 4$, $M(4) = 3$, and $M(i) = i$ for $i \neq 3, 7, 4$. Thus $M = (374)$.

The following theorem shows that applying a move to a configuration is compatible with multiplication in S_{16} when the move and configuration are both written as permutations.

Theorem 2.5. *In the 15-puzzle, applying a move M to a configuration C changes the puzzle's configuration into the product MC when M and C are interpreted as permutations in S_{16}.*

Proof. Pick $i \in \{1, \ldots, 16\}$. Viewing M and C as elements of S_{16}, $(MC)(i) = M(C(i))$. Since M is a move, the number $M(C(i))$ is the position in the puzzle to which M moves the piece in position $C(i)$. Since C is a configuration of the pieces, the number $C(i)$ is the position of piece i for configuration C. Therefore $M(C(i))$ is the position to which M moves piece i from configuration C. That is, $(MC)(i)$ is the position of piece i after applying move M to configuration C, for all i, so MC is the configuration of the puzzle after applying move M to configuration C. $\square$

Since Theorem 2.5 shows the multiplication of a move and a configuration of the 15-puzzle is the new configuration after the move, if we apply moves $M_1, M_2, \ldots, M_r$ in that order to a configuration C then the final configuration of the puzzle is the product $M_r \cdots M_2 M_1 C$.

Example 2.6. We saw in Example 2.4 that the move in (2.3) as a permutation is $M = (374)$. The initial configuration C in (2.3), as a permutation, is described in Example 2.2. The product $MC = (3\ 7\ 4)(1\ 6\ 7\ 9\ 13\ 16\ 8)(2\ 3\ 15\ 12)(4\ 14\ 10\ 11\ 5)$ is the 16-cycle

$$(1\ 6\ 4\ 14\ 10\ 11\ 5\ 3\ 15\ 12\ 2\ 7\ 9\ 13\ 16\ 8).$$

As a configuration, this says piece 1 is in position 6, piece 6 is in position 4, and so on up to piece 8 being in position 1, which is the final configuration in (2.3).

The four moves in (2.4), which affect positions 3, 4, 7, and 8, are successively (78), (37), (34), and (48). Their product in the opposite order is $(48)(34)(37)(78) = (374)(8) = (374)$, which is the permutation we found for the move in (2.3) at the end of Example 2.4. Multiplying in the other order, $(78)(37)(34)(48) = (347) \neq (374)$. Successive move permutations should be multiplied the way functions compose: from right to left.

Now we can explain why Sam Loyd's $1000 challenge can have no winner.

Theorem 2.7. *It is impossible to pass between* (2.1) *and* (2.2) *by sliding the pieces.*

Proof. Going from (2.1) to (2.2) and *vice versa* are equivalent. We focus on (2.1) to (2.2).

Each basic move of the 15-puzzle involves an exchange of positions between piece 16 (the empty space) and an actual piece. If pieces in positions i and j are swapped and other pieces stay put, that move is described by the permutation (ij) (no matter what pieces are in positions i and j). The permutation for the configuration (2.1) is the identity $C = (1)$ and the permutation for the configuration (2.2) is the transposition $C' = (14\ 15)$, so going from (2.1) to (2.2) in the 15-puzzle means there are some transpositions $\tau_1, \tau_2, \ldots, \tau_r$ in S_{16} such that $C' = \tau_r \cdots \tau_2\tau_1 C$. Since $C = (1)$ and $C' = (14\ 15)$ in S_{16},

$$(14\ 15) = \tau_r \cdots \tau_2\tau_1. \tag{2.5}$$

Because the empty space is in the same location in (2.1) and (2.2), after all the moves are carried out the empty space had to move up and down an equal number of times, and right and left an equal number of times. Since the empty space changes position by each τ_i, the number of transpositions on the right side of (2.5) is *even*. Therefore the right side of (2.5) is a product of an even number of transpositions, but the left side has an odd number of transpositions. This is a contradiction, so we are done. □

Remark 2.8. A more intuitive approach to Theorem 2.7 is to say each basic move in the puzzle involves piece 16, and if a sequence of moves interchanges piece 16 with pieces $a_1, a_2, \ldots, a_r$ then a more explicit version of (2.5) is $(14\ 15) = (a_r\ 16) \cdots (a_2\ 16)(a_1\ 16)$, with r being even since piece 16 moves an even number of times. That intuition is *not compatible* with Theorem 2.5, where a move is described as a permutation of the underlying *positions* it affects, not as a permutation of the specific numbered *pieces* involved. A succession of moves involving piece 16 is not expressed in Theorem 2.5 as a product of transpositions all involving (position) 16. If we model the effect of the moves in (2.4) as $(6\ 16)(5\ 16)(2\ 16)(6\ 16)$, which is (256), this tells us each piece is *replaced by* the next piece: 2 by 5, 5 by 6, and 6 by 2.

Corollary 2.9. *Every movement of pieces in the* 15*-puzzle starting from the standard configuration* (2.1) *that brings the empty space back to its original position must be an even permutation of the other* 15 *pieces.*

Proof. Let π be the permutation describing the configuration after the movement. Then π is also the permutation describing the move from the standard configuration: initially piece i is in position i, so $\pi(i)$ is where piece i winds up. Running through the proof of Theorem 2.7, with (14 15) replaced by π, from $\pi(16) = 16$ we get that π is an even permutation in S_{16}. Since $\pi(16) = 16$, we can view π in S_{15}. The parity of a permutation in S_{15} is the same as its parity when viewed as a permutation in S_{16} that fixes 16, so π is an even permutation of $1, 2, \ldots, 15$. □

The number of permutations of 15 objects is $15! = 1307674368000$. The number of even permutations of 15 objects is $15!/2 = 653837184000$. By Corollary 2.9, $15!/2$ is an upper bound on the number of (legal) positions of the pieces in the 15-puzzle with the empty space in the lower right. Is this bound achieved? Using 3-cycles we'll show the answer is yes.

Theorem 2.10. *For $n \geq 3$, A_n is generated by the 3-cycles $(1\ 2\ i)$ for $3 \leq i \leq n$.*

This is a standard result in group theory and we omit the proof.[3] It is a refinement of the more widely familiar fact in group theory that A_n is generated by *all* 3-cycles when $n \geq 3$.

Each basic move in the 15-puzzle involves the empty space, and two puzzle moves can't be composed unless the first one leaves the empty space where the second one needs it. Each configuration of the 15-puzzle can be modified to have the empty space in position 16, so we focus on moves that *leave the empty space in position* 16 *before and after the move.* Such moves, as permutations, are a subgroup of S_{16} and in fact S_{15}. Call it the 15-puzzle group, denoted as F. Its elements are even (Corollary 2.9), so F is a subgroup of A_{15}.

Theorem 2.11. *The* 15*-puzzle group F is A_{15}.*

Proof. We will use Theorem 2.10 in a "coordinate-free" form: A_{15} is generated by 3-cycles involving a common pair of terms. We will use the 3-cycles $(11\ 12\ i)$ instead of $(1\ 2\ i)$.

The move $M = (11\ 12\ 15)$ can be realized as follows, using i in position i for clarity.

$$\begin{array}{|c|c|}\hline 11 & 12 \\ \hline 15 & \\ \hline\end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 11 & \\ \hline 15 & 12 \\ \hline\end{array} \rightsquigarrow \begin{array}{|c|c|}\hline & 11 \\ \hline 15 & 12 \\ \hline\end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 15 & 11 \\ \hline & 12 \\ \hline\end{array} \rightsquigarrow \begin{array}{|c|c|}\hline 15 & 11 \\ \hline 12 & \\ \hline\end{array} \tag{2.6}$$

Thus $M \in F$. For each $i \neq \{11, 12, 15, 16\}$, we will find g_i in F carrying the piece in position i to position 15 (so $g_i(i) = 15$) while leaving pieces in positions 11, 12, and 16 fixed. Then $g_i^{-1} M g_i = (g_i^{-1}(11)\ g_i^{-1}(12)\ g_i^{-1}(15)) = (11\ 12\ i)$, so $(11\ 12\ i) \in F$ for all $i \neq 11, 12, 16$.

Starting in the standard configuration (2.1), let m be the move taking the empty space to the inside of the puzzle by exchanging it with 12 and then 11, as shown below.

$$\begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 \\ \hline 9 & 10 & 11 & 12 \\ \hline 13 & 14 & 15 & \\ \hline\end{array} \overset{m}{\rightsquigarrow} \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 \\ \hline 9 & 10 & & 11 \\ \hline 13 & 14 & 15 & 12 \\ \hline\end{array}$$

As a permutation in S_{16}, $m = (11\ 12\ 16)$. This is not in F since position 16 is not fixed.

Below are two 'tours' that together make the rest of the board pass through the empty space and the 15 in the configuration on the right side above. In the figures below, each tour is highlighted in bold and we use 16 as a label for the empty space. These tours are 16,7,3,2,1,5,9,13,14,15 on the left and 16,7,8,4,3,2,6,10,14,15 on the right.

$$\begin{array}{|c|c|c|c|}\hline \mathbf{1} & \mathbf{2} & \mathbf{3} & 4 \\ \hline \mathbf{5} & 6 & \mathbf{7} & 8 \\ \hline \mathbf{9} & 10 & \mathbf{16} & 11 \\ \hline \mathbf{13} & \mathbf{14} & \mathbf{15} & 12 \\ \hline\end{array} \qquad \begin{array}{|c|c|c|c|}\hline 1 & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \hline 5 & \mathbf{6} & \mathbf{7} & \mathbf{8} \\ \hline 9 & \mathbf{10} & \mathbf{16} & 11 \\ \hline 13 & \mathbf{14} & \mathbf{15} & 12 \\ \hline\end{array}$$

(I found these in [3, pp. 123–124], which is all about permutation puzzles.) For each $i \neq 11, 12, 16$, one of the tours gives us a move h_i that brings piece i from position i to position 15, by backtracking keeps the empty space 16 in position 11, and doesn't change the pieces 11 and 12 in positions 12 and 16. So as a permutation, h_i fixes 11, 12, and 16, and $h_i(i) = 15$. Since the 3-cycle $m = (11\ 12\ 16)$ fixes i and 15, the reader can check that the move $g_i = m^{-1} h_i m$ fixes positions 11, 12, and 16 (it lies in F), and $g_i(i) = 15$. It

[3]See Theorem 3.3 in https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf.

follows, as explained earlier, that $(11\ 12\ i) \in F$. As i varies such 3-cycles generate A_{15}, so $F = A_{15}$. $\square$

This completes the analysis of the 15-puzzle: exactly half the permutations of the pieces 1 through 15 can be reached from the standard configuration, since A_{15} is generated by the 3-cycles with a common pair of terms, such as 11 and 12.

Example 2.12. We will determine if the configuration

(2.7)

8	7	6	5
9	3	1	10
2	11	14	4
12	15	13	

can be reached from (2.1). The permutation for the move from (2.1) to (2.7) sends each i (the piece in position i in (2.1)) to the position of i in (2.7). That is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 7 & 9 & 6 & 12 & 4 & 3 & 2 & 1 & 5 & 8 & 10 & 13 & 15 & 11 & 14 \end{pmatrix},$$

which when written as a product of disjoint cycles becomes

$$(1\ 7\ 2\ 9\ 5\ 4\ 12\ 13\ 15\ 14\ 11\ 10\ 8)(3\ 6).$$

This is a 13-cycle times a 2-cycle. A 13-cycle is an even permutation and a 2-cycle is an odd permutation, so overall this move is an odd permutation. Therefore it is impossible to reach (2.7) from (2.1), or conversely to go from (2.7) to (2.1).

3. Rubik's Cube

Nothing like the 19-th century frenzy over the 15-puzzle was seen again until essentially 100 years later, when Rubik's Cube came on the scene in the early 1980s. Its inventor, Erno Rubik, became the first self-made millionaire in the Communist bloc.

It's best if you have a copy of the cube to play with as you read the remaining discussion. We will *not* describe a solution to the cube, although you can find some on the internet that don't require too much memorization. (Such a method in book form is in [2, Chapter 3].) What we will do here is introduce enough notation and terminology to explain what the group of all permutations of Rubik's Cube is, much like the group of all permutations of the 15-puzzle (preserving the empty space in the bottom right corner) is A_{15}.

If you use a screwdriver to carefully pop out a piece along an edge (see Figures 2 and 3) then the rest of the pieces easily come out and the interesting center mechanism is revealed (Figure 4). This shows a basic fact about the cube: the 6 center pieces are actually one single piece and no amount of turning will ever change the relative positions of the center faces. Because the center pieces always maintain the same relative positions, each central color tells you what color that whole face must be in the solved cube. For instance, if a messed up cube has blue and green as opposite center colors then the solved state of that cube will have blue and green faces opposite each other.

There are three kinds of pieces in the cube: 8 corner pieces (each with 3 stickers), 12 edge pieces (each having 2 stickers) and 6 center pieces (each with one sticker). See Figure 5. The number of non-center stickers is $8 \cdot 3 + 12 \cdot 2 = 48$. When you make a move of the cube, the 3 colors on a corner stay together and the 2 colors on an edge stay together.

Although you can physically rotate the whole cube in space to get a better view, this is not a move: relative positions of each piece stay the same. To discuss constraints on

FIGURE 2. Beginning to disassemble the cube along an edge.

FIGURE 3. One edge piece out.

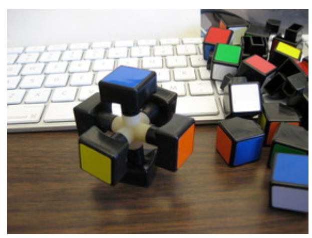

FIGURE 4. The center mechanism.

FIGURE 5. A corner and edge piece.

what can be done on a Rubik's Cube, center pieces can be kept in fixed positions (no cube rotations). When holding the cube with one face facing you, the labels of the 6 faces are

- F for Front,
- B for Back,
- L for Left,
- R for Right,
- U for Up,
- D for Down.

See Figure 6. The labels Up/Down are used instead of Top/Bottom to avoid confusion over the meaning of B (Bottom or Back?) I have seen a book on Rubik's Cube that uses the labels Top/Bottom, and calls the Back face the P(osterior) face, but this is uncommon. The face labels we use here, due to D. Singmaster, are essentially universally accepted[4].

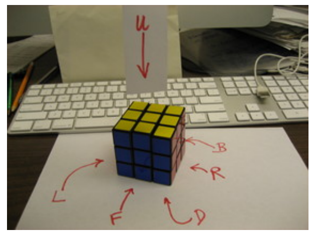

FIGURE 6. Face Names.

Below is a diagram of the cube unfolded, taken from [3, p. 72]. (The numbers $1, 2, \ldots, 48$ correspond to non-center stickers.) In this standard configuration, sticker i is in position i.

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

The labels F, B, L, R, U, D are used in two ways: to mark each face's center (which does not move), and to denote a quarter-turn clockwise of that face if you look at it head-on in a natural way. If you hold a cube with F in front of you (and U lying above it) then

- F is a quarter-turn of the Front face carrying its top row to R,
- B is a quarter-turn of the Back face carrying its top row to L,
- L is a quarter-turn of the Left face carrying its top row to F,
- R is a quarter-turn of the Right face carrying its top row to B,
- U is a quarter-turn of the Up face carrying its front row to L,
- D is a quarter-turn of the Down face carrying its front row to R.

[4]The colors on the cube are not universally standardized among different manufacturers. Even cubes with the same 6 face colors can have them appear in different positions: white may be opposite blue on one solved cube but be opposite red on another solved cube. This is why it is important to refer to arrangements of pieces on the cube using a notation that is color independent, like Singmaster's notation.

We call these 6 quarter-turns the *basic* moves of the cube. Another natural class of moves is quarter-turns of the three middle layers, which can be accounted for with basic moves since a quarter-turn of a middle layer in one direction is the same as quarter-turns of the two parallel outer layers in the opposite direction, and that is a product of two of the six basic moves above.

Referring to the cube-face diagram above, a tedious verification shows the 6 basic moves are the following elements of S_{48}, where for each move M, $M(i)$ is the position where M sends i from the standard configuration. (More abstractly, for each configuration, $M(i)$ is the position where M moves the piece in position i.)

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

From a group-theoretic perspective, understanding all possible configurations of a Rubik's Cube amounts to asking: what subgroup of S_{48} is generated by F, B, L, R, U, D:

$$\langle \mathrm{F, B, L, R, U, D} \rangle = ???.$$

This set of all products of permutations generated by the 6 moves is called Rubik's group. Can it be written down in terms of simpler known groups? This is comparable to the connection between the arrangements of the pieces in the 15-puzzle and the group A_{15}.

Since corner and edge pieces can never occupy each other's positions, thinking about Rubik's group inside S_{48} is not such a great idea. We should consider the corner and edge pieces separately. However, although each move of the cube permutes the 8 corner pieces among themselves and the 12 edge pieces among themselves, there is more information in a move than how it permutes the corner pieces and how it permutes the edge pieces: each corner and edge piece has an *orientation*, describing how it fits into its current position.

We call a position that a corner or edge piece can be placed in a *cubicle*. There are 20 of them: 8 corner cubicles and 12 edge cubicles. A corner cubicle can be filled by a corner piece in 3 ways, while an edge cubicle can be filled by an edge piece in 2 ways. These different possibilities are called the orientations of the (corner or edge) piece. We call the pieces in the solved state of the cube 'oriented.' How can we decide if the pieces are oriented or not in other states of the cube?

Each corner piece has one color matching the center color of the U or D face, since in the solved state the corner has this property. Mark that face of the corner. On the edge pieces having a color belonging to U or D, mark that face of the edge. On the edge pieces not having a color belonging to U or D, there will be a color belonging to F or B. Mark that face. We have now marked one face of each corner piece and each edge piece.

If you play with the cube, remembering not to change the location of the center pieces (that is, don't rotate the whole cube in space), after the pieces are scattered about the cube we can assign a corner piece and edge piece an *orientation* value that is in $\mathbf{Z}/(3)$ for corners and in $\mathbf{Z}/(2)$ for edges according to the following rules:

- If a corner piece has its marked color on the U or D face, give the piece orientation value 0. (A corner piece will never be in the middle layer.) If a corner piece has its marked color not on its U or D face, that color can be brought to the U or D face by a 1/3 rotation (in your mind!) either clockwise or counterclockwise. If we can bring the marked color to the U or D face with a clockwise 1/3 rotation, give the piece orientation value 1. Otherwise we can bring the marked color to the U or D face with a counterclockwise 1/3 rotation and we give the piece orientation value -1. (Thus, in all cases, an orientation value of n on a corner piece means a clockwise rotation by $2\pi n/3$ radians will put the marked color of the piece on the U or D face.)
- If an edge piece is in the upper or lower layer of the cube and has its marked color on the U or D face, give the piece orientation value 0. If the piece is in the middle layer and its marked color is on the F or B face, give the piece orientation value 0. In other cases give the piece orientation value 1.

Instead of viewing a move of the cube in S_{48} (as a permutation of the stickers) we can view it as a permutation of the 8 corner pieces, keeping track of the 3 orientation values for each corner piece, and a permutation of the 12 edge pieces, keeping track of the 2 orientations of each edge piece. (That is still $8 \times 3 + 12 \times 2 = 48$ pieces of information.) Give the corner pieces a definite labeling $1, 2, \ldots, 8$ and the edge pieces a definite labeling $1, 2, \ldots, 12$. Then each move of the cube corresponds to a choice of 4-tuple from

$$S_8 \times S_{12} \times (\mathbf{Z}/(3))^8 \times (\mathbf{Z}/(2))^{12}. \tag{3.1}$$

Which 4-tuples $(\pi, \rho, \mathbf{v}, \mathbf{w})$ from this set really correspond to moves on the cube? There are a few constraints. First of all, as a permutation on the pieces, each move among F, B, L, R, U, D is a 4-cycle on the 4 corner pieces it moves and a 4-cycle on the 4 edge pieces it moves. A 4-cycle is odd, so each basic move gives an odd permutation in S_8 and in S_{12}. This might sound strange: odd permutations do not form a group! However, let's think about the fact that *both* of the permutations of corner and edge pieces in F, B, L, R, U, or D are odd. When composed, permutations with this feature will have both odd or both even effects on the corner and edge pieces. In other words, two permutations $\pi \in S_8$ and $\rho \in S_{12}$ coming from the same move of the cube satisfy

$$\operatorname{sgn}(\pi) = \operatorname{sgn}(\rho). \tag{3.2}$$

As for the orientations, a computation shows that each basic move does not change the sum of the coordinates in the orientation vectors $\mathbf{v}$ and $\mathbf{w}$ for a particular arrangement of the pieces. Thus, since a solved cube has both orientation vectors equal to $\mathbf{0}$, an actual move of the cube must have

$$\sum_{i=1}^{8} v_i \equiv 0 \bmod 3, \quad \sum_{j=1}^{12} w_j \equiv 0 \bmod 2. \tag{3.3}$$

(The first formula in (3.3) tells us that in a move of the cube, we can't change the orientation of a single corner piece without changing something else. Similarly, the second formula in (3.3) tells us no move of the cube can change the orientation of a single edge piece without changing something else. A single corner rotation would change $\sum_{i=1}^{8} v_i \bmod 3$ by $\pm 1 \bmod 3$, which doesn't preserve the condition $\sum_{i=1}^{8} v_i \equiv 0 \bmod 3$.)

The conditions (3.2) and (3.3) carve out the following subset of (3.1):

$$\left\{(\pi,\rho,\mathbf{v},\mathbf{w}) : \operatorname{sgn}\pi = \operatorname{sgn}\rho,\ \sum_{i=1}^{8} v_i \equiv 0 \bmod 3,\ \sum_{j=1}^{12} w_j \equiv 0 \bmod 2\right\}. \tag{3.4}$$

Every arrangement of the pieces in Rubik's Cube that can be reached from the solved state lies in (3.4). It turns out that, conversely, every 4-tuple in (3.4) is a solvable arrangement of the pieces in Rubik's Cube. This is shown in [1, p. 42], which gives an (inefficient) algorithm to solve the cube starting from an arbitrary configuration satisfying (3.4). Therefore the number of arrangements of the pieces in Rubik's Cube is the size of (3.4). How large is (3.4)? Among all pairs of permutations $(\pi,\rho) \in S_8 \times S_{12}$, *half* have $\operatorname{sgn}\pi = \operatorname{sgn}\rho$. Among the 8-tuples $\mathbf{v} \in (\mathbf{Z}/(3))^8$, *one-third* have the sum of coordinates equal to 0. Among the 12-tuples $\mathbf{w} \in (\mathbf{Z}/(2))^{12}$, *half* have the sum of coordinates equal to 0. So the total number of arrangements of the pieces in Rubik's Cube that you get by mixing it up without taking it apart is

$$\frac{8!12!3^8 2^{12}}{2\cdot 3\cdot 2} = 2^{27}3^{14}5^3 7^2 11 = 43252003274489856000 \approx 4.3\cdot 10^{19}. \tag{3.5}$$

This size is impressive, but its magnitude should not be construed as a reason that Rubik's Cube is hard to solve. After all, the letters of the alphabet can be arranged in $26! \approx 4.03\cdot 10^{26}$ ways but it is very easy to rearrange a listing of the letters into alphabetical order. If a company came out with the Alphabet Game and said on the packaging "Over 4×10^{26} possibilities!" you would not think it must be hard since that number is so big.

The denominator $2\cdot 3\cdot 2 = 12$ in (3.5) comes from the three constraints in (3.4). If you were to take apart the cube and put it back together at random, it is possible you wouldn't be able to solve it. In fact, the probability is only $\frac{1}{12}$ that you can solve it, because a random choice of $(\pi,\rho,\mathbf{v},\mathbf{w})$ will have all three conditions in (3.4) satisfied with probability $\frac{1}{2}\cdot\frac{1}{3}\cdot\frac{1}{2} = \frac{1}{12}$. You won't be able to solve it if $\operatorname{sgn}\pi \neq \operatorname{sgn}\rho$, if $\sum v_i \equiv 1, 2 \bmod 3$, or if $\sum w_j \equiv 1 \bmod 2$.

Viewing (3.1) as a direct product of four groups, (3.4) is a subgroup, since the defining conditions are preserved under componentwise operations. Is (3.4), as a subgroup of a direct product group, the group of permutations of Rubik's Cube? No. Componentwise operations in (3.1) do not match the way moves of the cube in (3.4) compose with one another. Another group structure on (3.1) reflects how moves of the cube compose:

$$(\pi,\rho,\mathbf{v},\mathbf{w})(\pi',\rho',\mathbf{v}',\mathbf{w}') = (\pi\pi',\rho\rho',\mathbf{v}+\pi\mathbf{v}',\mathbf{w}+\rho\mathbf{w}'). \tag{3.6}$$

(The notation $\pi\mathbf{v}'$ means the vector in $(\mathbf{Z}/(3))^8$ obtained by permuting the 8 coordinates of $\mathbf{v}'$ according to the permutation $\pi \in S_8$. The meaning of $\rho\mathbf{w}'$ as a vector in $(\mathbf{Z}/(2))^{12}$ is similar.) The operation (3.6) is componentwise in the first two coordinates, but not in the last two coordinates. This "twisted" direct product operation is called a *semi-direct product*. The set (3.4) with the composition law (3.6) is a group, because permuting coordinates of a vector does not change the sum of the coordinates. A proof that this is the group of movements of the pieces in Rubik's Cube is in [1, pp. 47–48].

In addition to disassembling the cube with a screwdriver in order to solve it, you could peel off the stickers and put them back on the faces in a solved state. This is actually a really awful idea, because the adhesive holding the stickers onto the faces is seriously weakened by peeling. But let's think about the mathematical problem raised by this method: if you peel off all the non-center stickers and put them back on at random, what is the probability you would be able to solve the cube?

The probability turns out to be *much smaller* than the $\frac{1}{12}$ probability of solving the cube after taking the cube apart with a screwdriver and randomly reassembling the pieces. That is, there are far more ways to make a cube unsolvable by peeling and resticking. For instance, putting two stickers of the same color on both faces of an edge piece makes the cube impossible to solve no matter what else is done with the other stickers. Other ways of making a cube unsolvable with bad color combinations on a corner piece or edge piece are easy to imagine. (By comparison, if you use the screwdriver method of disassembly and reassembly, placing an edge into the cube in a misoriented way can be counterbalanced by putting in another edge in a misoriented way.)

To compute the probability of solving a cube after a random resticking of non-center faces, we know the number of solvable states of the cube (with center colors fixed) is given by (3.5). The number of ways to place the 48 non-center colors onto the faces after peeling is 48!. We can't tell the difference between restickings that differ by permutations of stickers with the same color. Each of the 6 colors is on 8 non-center faces, so every particular resticking can occur in $8!^6$ ways. So the probability that peeling off the non-center faces and randomly putting them back on the cube will be a solvable cube is

$$\frac{(8!12!3^8 2^{12}/12)(8!^6)}{48!} \approx 1.49 \cdot 10^{-14},$$

which is far smaller than $\frac{1}{12}$.

Suppose we now allow complete freedom: even the center stickers can be removed. There are 54! ways of putting all 54 stickers back onto the cube and each particular resticking can be done in $9!^6$ ways since permuting the stickers with a fixed color doesn't change the appearance of the faces. For a resticking to be a solvable cube, the center faces have to be assigned different colors. That can be done in 6! ways (no specification of which sticker of each color is actually used). If such an assignment of the center faces is made, there are $8!12!3^8 2^{12}/12$ ways to restick the remaining stickers into a solvable state of the cube. The probability that a resticking of all the stickers is a solvable state of the cube is therefore

$$\frac{(8!12!3^8 2^{12}/12)(6!)(9!^6)}{54!} \approx 3.08 \cdot 10^{-16}.$$

References

[1] C. Bandelow, *Inside Rubik's Cube and Beyond*, Birkhäuser, 1982.

[2] A. H. Frey, Jr. and D. Singmaster, *Handbook of Cubic Math*, Enslow Publishers, 1982.

[3] D. Joyner, *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*, Johns Hopkins Univ. Press, 2002.

[4] J. Mulholland, *Permutation Puzzles: A Mathematical Perspective*, `http://www.sfu.ca/~jtmulhol/math302/notes/302notes.pdf`.

[5] J. Slocum and D. Sonneveld, *The 15-Puzzle Book*, Slocum Puzzle Foundation, 2006.