MATHEMATICAL APPROACH TO RUBIK'S CUBE

Project submitted to the University of Kerala, Thiruvananthapuram in partial fulfillment of the requirement for the award of the Degree of Bachelor of Science in Mathematics under CBCSS

Submitted by

Devika B **22021104029**

Examination Code	**: 22018604**
Subject Code	**: MM 1646**
Year of Study	**: 2021-2024**
Guided by	**: Dr.Rejitha K R**

DEPARTMENT OF MATHEMATICS

KSMDB COLLEGE SASTHAMCOTTA, KOLLAM

2021-2024

CERTIFICATE

This is to certify that the thesis entitled "MATHEMATICAL APPROACH TO RUBIK'S CUBE" submitted to the University of Kerala in partial fulfillment of the requirement of the BSc Degree in Mathematics is a record of bonafied research carried out by **Devika B** of this department.

Head of the Department
Dr.Savitha M T

Supervising Teacher
Dr.Rejitha K R

Examiner

Sasthamcotta
April 2024

2/5/24

ACKNOWLEDGEMENT

I express my deep sense of gratitude to Dr.Rejitha K R, Assistant Professor, K.S.M.D.B.College, Sasthamcotta for her excellent guidance, suggestions, and valuable support for the completion of my project successfully. I also express my indebtedness and extreme gratitude to my teachers in the Department of Mathematics for their helpful guidance and supervision, which enabled me to complete this work successfully. I also like to thank the library staff of Kumbalathu Sanku Pillai Memorial Devaswom Board College, Sasthamcotta for their services and my friends who helped me to complete this project work.

Devika B

DECLARATION

I hereby declare that the thesis represents my work done for the partial fulfillment of the degree of BSc Mathematics at KSMDB College, affiliated with Kerala University. This work carried out by me and it has not been submitted earlier or elsewhere for similar purposes according to the best of my knowledge and belief.

Devika B

Contents

Introduction

"We turn the Cube and it twists us."- Erno Rubik

The Rubik's Cube is a 3-D mechanical puzzle originally called the "Magic Cube", invented in 1974 by Erno Rubik. He is a Hungarian inventor, architect, and professor of architecture. This game aims to bring all the colors to the same side.

In the mid-1970s, Erno Rubik worked at the Department of Interior Design at the Academy of Applied Arts and Crafts in Budapest. Although it was widely reported that the cube was built as a teaching tool to help his students understand 3D objects, his actual purpose was solving the structural problem of moving the parts independently without the entire mechanism falling apart. He did not realize that he had created a puzzle until the first time he scrambled his new Cube and then tried to restore it. Rubik applied for a patent in Hungary for his "Magic Cube" (Hungarian: Büvös kocka) on 30 January 1975. The first test batches of the Magic Cube were produced in late 1977 and released in Budapest toy shops. Magic Cube was held together with interlocking plastic pieces that prevented the puzzle from being easily pulled apart, unlike the magnets in Nichols's design. With Erno Rubik's permission, businessman Tibor Laczi took a Cube to Germany's Nuremberg Toy Fair in February 1979 in an attempt to popularize it. It was

noticed by Seven Towns founder Tom Kremer, and they signed a deal with Ideal Toys in September 1979 to release the Magic Cube worldwide. Ideal wanted at least a recognizable name to trademark. That arrangement put Rubik in the spotlight because the Magic Cube was renamed after its inventor in 1980. The puzzle made its international debut at the toy fairs of London, Paris, Nuremberg, and New York in January and February 1980.

After its international debut, the progress of the Cube towards the toy shop shelves of the West was briefly halted so that it could be manufactured to Western safety and packaging specifications. A lighter Cube was produced, and Ideal decided to rename it. "The Gordian Knot" and "Inca Gold" were considered, but the company finally decided on "Rubik's Cube", and the first batch was exported from Hungary in May 1980.

There are several connections one can make between the Rubik's Cube and math. The Rubik's Cube can be used to conceptualize surface area and volume, as well as exhibit a net of a familiar, three-dimensional solid. The Rubik's Cube can be connected to fractions, ratios, and proportional reasoning.

In this project, we are concerned with the study of **Mathematical Approach to Rubik's Cube**. In the first chapter, we deal with the basic definitions related to our field of study. In the second chapter, we will move deep into the concept of the Rubik's Cube, In the third chapter we will discuss about the Rubik's cube and word problems, and the fourth chapter we will study different methods of solving the cube.

Chapter 1

Preliminaries

1.1 Basic Definitions

Definition 1.1.1. Groups : Let G be a non-empty set, $*$ be a binary operation on G. Then $(G, *)$ is said to be a group if $*$ satisfies the following properties:

1. The operation * is closed. So for any group elements h and g in G, $h * g$ is closed under *.

2. The operation $*$ is associative. So for any elements f, g and $h, f * (g* h) = (f * g) * h, \forall f, g, h \in G$.

3. There exist an identity element $e \in G$ such that $e * g = g * e = g$, $\forall g \in G$.

4. For every element $g \in G$, there exist an inverse $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

1.1.1. Theorems About Groups

The basic group theorems are :

1. The identity element e, is unique.
2. If $a * b = e$, then $a = b^{-1}$.
3. If $a * x = b * x$, then $a = b$.
4. The inverse of (ab) is $b^{-1}a^{-1}$.
5. $(a^{-1})^{-1} = a$

1.1.2.Examples of Groups

Some of the common examples of groups are:

- The integers form a group under addition. The identity element is 0, and the inverse of any integer a is its negative, $-a$.
- The non-zero rational numbers form a group under multiplication. The identity element is 1, and the inverse of any x is $\frac{1}{x}$.
- The set of $n \times n$ non-singular matrices form a group under multiplication. This is an example of a non-commutative group or non-abelian group.

Definition 1.1.2. Inverses: The inverse of an element $g \in G$ is written as g^{-1}. If g and h are two elements of a group, then $(hg)^{-1} = g^{-1}h^{-1}$.

Definition 1.1.3. Concatenation: A group of things linked together or occurring together in a way that produces a particular result or effect.

Definition 1.1.4. Permutation: An arrangement of objects in a definite order.

Definition 1.1.5. Cycle: An expression of the form $a_1, a_2, \ldots, a_m$ is called a cycle.

Definition 1.1.6. Canonical cycle notation: A unique way of writing a permutation as a product of disjoint cycles.

Definition 1.1.7. Transposition: A cycle of length two is called transposition.

Definition 1.1.8. Cosets: A subset of a mathematical group that consists of all the products obtained by multiplying either on the right or the left a fixed element of the group by each of the elements of a given subgroup.

Definition 1.1.9. Order: Let G be a group, $a \in G$, then the order of ' a ' in G is denoted by $O(a)$ or $|a|$ and is defined as the least positive integer n such that $a^n = e$.

Definition 1.1.10. Commutator: An element of a mathematical group that when used to multiply the product of two given elements either on the right side or on the left side but not necessarily on both sides yields the product of the two given elements in reverse order. The commutator indicates the extent to which a certain binary operation fails to be commutative.

Definition 1.1.11. Conjugation: Conjugation defines a group action of a group on itself. Suppose G is a group. Two elements a and b of G are called conjugate if there exists an element g in G with $g * a * g^{-1} = b$. Here $*$ is the binary operation on the group.

Definition 1.1.12. Equivalence Class: It is the name given to the subset of a set S which includes all elements that are equivalent to each other.

Chapter 2

Group Theory on Rubik's cube

2.1 Rubik's Cube

Rubik's cube is a mind game. In a classic Rubik's cube, each of the six faces is covered by nine stickers, among six solid colors. Traditionally:

- Red
- White
- Blue
- Orange
- Green
- Yellow

A standard Rubik's cube measures 5.7 cm (approximately $2\frac{1}{4}$ inches) on each side. The puzzle consists of 26 unique miniature cubes, also called "cubies" or "cubelets".

2.2 Notation

Throughout this chapter, we will be using the following notation to refer to the sides of the cube as shown in Figure 2.1.

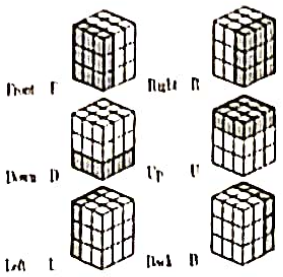


Figure 2.1: Notation

A counterclockwise rotation is denoted by lowercase letters (f) or by adding an apostrophe (F'). A 180-degree turn is denoted by adding a superscript 2 (F^2), or just a move followed by a 2($F2$).

To refer to an individual cubie or a face of a cubie, we use one letter for the center cubies, two letters for the edge cubies, and three letters for the corner cubies, which give the faces of the cube that the cubie is part of. The first of the three letters give the side of the cubie we are referring to.

2.3 Rubik's Cube Group

On the Rubik's Cube, 54 facets can be arranged and rearranged by twisting and turning the faces. Any position of the cube can be described as a permutation from the solved state. Thus, the Rubik's Cube group is a subgroup of a permutation group of 54 elements.

Rubik's Cube Group: The permutation group $G = \langle F, L, U, D, R, B \rangle \subset S_{54}$ is called the Rubik's Cube Group.

There are two different classifications of the Rubik's Cube Group: the Legal Rubik's Cube Group and the Illegal Rubik's Cube Group. The difference between the two is that the Illegal Rubik's Cube Group allows the solver to take the cube apart and rearrange the facets. In neither case is the solver allowed to remove the stickers from each facet. As expected, the Rubik's Cube Group is a subset of the Illegal Rubik's Cube group.

Now, not all of the permutations of S_{54} will be possible on the Rubik's Cube. The middle facet on each side of the cube is fixed and cannot be permutated to a different position on the cube. Furthermore, any valid permutation on the cube will send corner facets to corner positions and edge facets to edge positions. Any other permutations will not be physically possible on the cube. Hence, G is only a subset of S_{54} and not isomorphic to the full permutation group.

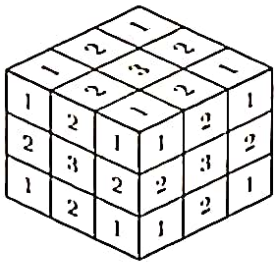


Figure 2.2

The different types of facets on a Rubik's Cube: 1 denotes the facets that makeup corner cubes, 2 denotes facets that makeup edge cubes and 3 denotes the fixed center cubes

2.4 Bounds on Solving a Rubik's Cube

The number of possible permutations of the squares on a Rubik's cube seems challenging. Eight corner pieces can be arranged in 8! ways, each of which can be arranged in three orientations, giving 3^8 possibilities for each permutation of the corner pieces. 12 edge pieces can be arranged in 12! ways. Each edge piece has 2 possible orientations, so each permutation of edge pieces has 2^{12} arrangements. But in the Rubik's cube, only $\frac{1}{3}$ of the permutations have the rotations of the corner cubies correct. Only $\frac{1}{2}$ of the permutations have the same edge-flipping orientation as the original cube, and only $\frac{1}{2}$ of these have the correct cubie rearrangement parity, which will be discussed later. This gives:

$$\frac{(8! \cdot 3^8 \cdot 12! \cdot 2^{12})}{(3 \cdot 2 \cdot 2)} = 4.3252 \cdot 10^{19}$$

possible arrangements of the Rubik's cube.

2.5 Cube Moves as Group Elements

We can represent the cube permutations as group elements. Let the group of permutations for Rubik's cube be represented as $\Re$.

2.5.1. The Binary Operator for the Rubik Group

Our binary operator $*$ will be a concatenation of sequences of cube moves, or rotations of a face of the cube. The symbol $*$ will almost be omitted and interpret fg as $f * g$. This operation is closed since any face rotation still leaves with a permutation of the cube, which is in $\Re$. Rotations are also associative. The

identity element e corresponds to not changing the cube at all.

2.5.2. Inverses

If F is the cube move that rotates the front face clockwise, then f, the inverse of F, moves the front face counterclockwise. Suppose there is a sequence of moves, say FR, then the inverse of FR is rf.

2.6 Permutations

The different move sequences of cube elements can be viewed as permutations, or rearrangements, of the cubies.

Note 2.6.1. Sequences that return the same cube configuration are seen to be the same element of the group of permutations. So every move can be written as a permutation. For example, the move F F RR is the same as the permutation (DF UF)(DR UR)(BR FR FL)(DBR UFR DFL)(ULF URB *DRF*).

An example of a permutation written in **canonical cycle notation** is:

(1)(234)

This means that 1 stays in place, and elements 2,3, and 4 are cycled. For example, 2 goes to 3,3 goes to 4 , and 4 goes to 2 . (234) → (423).

2.7 Parity

The evenness or oddness of a permutation is called parity. For example, (123)(56) = (12)(23)(56) has odd parity. Permutation can also be described in terms of their parity. Any cycle of n length of a permutation can be expressed as the product of 2 - cycles. The parity of a n length cycle is given by the number of 2 - cycles it is composed of. If n is even, an odd number of 2 - cycles is required, and the permutation is odd, and vice versa. Odd permutations end up exchanging an odd number of cubies, and even ones an even number.

Theorem 2.7.1. The cube always has even parity or an even number of cubies exchanged from the starting position.

Proof. Base case: After n = 0 moves on an unsolved cube, there are no cubies exchanged, and 0 is even.

Let $P(n)$: After n rotations, there are an even number of cubies exchanged. We assume $P(n)$ to show $P(n) \rightarrow P(n+1)$. Any sequence of moves is composed of single-face turns. As an example of the permutation created by a face turn, look at the move $F = (FLFUFRFD)(FULFURFDRFDL) = (FLFU)(FLFR)(FLFD)$ $(FULFUR)(FULFDR)(FULFDL)$. Since each of the length 4 chains in this permutation can be written as 32 - cycles for a total of 62 - cycles, the parity of the face turn is even. This fact applies to any face turn, since all face turns, no matter which face they are applied to, are essentially equivalent. After n moves the cube has an even number of cubies exchanged. Since the $n+1$ move will be a face turn, there will be an even number of cubies flipped. There was already an even number exchanged, and so an even parity of cubies exchanges is preserved overall.

Since any permutation of the Rubik's cube has even parity, no move will ex-

change a single pair of cubies. This means that when two cubies are exchanged, we know other cubies must also be exchanged. We will get around this problem by using 3-cycles that will cycle 3 cubies, including the two that we want to exchange.

2.8 Subgroups

Given a group $\mathfrak{R}$, if $S \subseteq \mathfrak{R}$, then the subgroup H generated by S is the smallest subgroup of $\mathfrak{R}$ that contains all the elements of S.

For example, $\{F\}$ generates a group that is a subgroup of $\mathfrak{R}$ consisting of all the possible cube permutations obtained by rotating the front face, i.e., $\{F, F^2, F^3, F^4\}$. The group generated by $\{F, B, U, L.R, D\}$ is the whole group $\mathfrak{R}$.

Here the term order is used to describe how many times we have to repeat a particular move before returning to the identity. For example, The move F generates a subgroup of order 4, since rotating a face 4 times returns to the original state. The move FF generates a subgroup of order 2.

Theorem 2.8.1. If the cube starts at the solved state, and one move sequence P is performed successively, the cube will eventually return to its solved state.

Proof. Let P be any cube sequence. Then at some number of times m that P is applied, it recycles to the same arrangement k, where $k < m$ and m is the soonest an arrangement appears for the second time. So $P^k = P^m$. Thus if we show that k must be 0, we have proved that the cube cycles back to P^0, the solved state.

If $k = 0$, then we are done, since $P^0 = 1 = P^m$. Now we prove by contradiction that k must be 0. If $k > 0$: if we apply P^{-1} to both P^k and P^m we get the same thing, since both the arrangements P^k and P^m are the same. Then $P^k P^{-1} =$

$P^m P^{-1} \Rightarrow P^{k-1} = P^{m-1}$. But this is contradictory since we said that m is the first time that arrangements repeat. So therefore k must equal 0 and every move sequence eventually cycles through the initial state again first before repeating other arrangements.

2.9 Lagrange's Theorem

If G is a group and H is a subgroup of G, then for an element g of G we define a coset as:

- $gH = \{gH : h \in H\}$ is a left coset of H in G.
- $Hg = \{gh : h \in H\}$ is a right coset of H in G.

The number of times the steps to be repeated on the move FFRR to get back to the starting position is six. No matter what, that number, the size of the subgroup generated by $FFRR$, must be a divisor of $\frac{(8!\cdot 3^8\cdot 12!\cdot 2^{12})}{(3\cdot 2\cdot 2)}$. It can be explained by Lagrange's theorem as follows:

If H is the subgroup of $\Re$ generated by F, then one right coset is shown below:

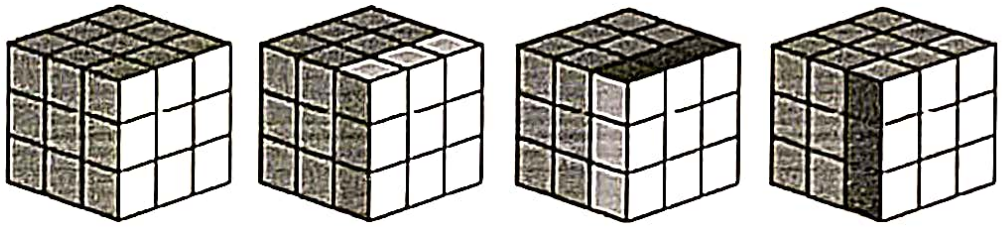


Figure 2.3:

Lemma 2.9.1. If H is a finite subgroup of a group G and H contains n elements, then any right coset of H contains n elements.

Proof. For any element $g \in G, Hg = \{hg \mid h \in H\}$ defines the right coset. There is one element in the coset for every h in H, so the coset has n elements.

Lemma 2.9.2. Two right cosets of a subgroup H in a group G are either identical or disjoint.

Proof. Suppose Hx and Hy have an element in common. Then for some h_1 and h_2 :

$$h_1 x = h_2 y$$

Then $x = h_1^{-1} h_2 y$, and some $h_3 = h_1^{-1} h_2$ gives $x = h_3 y$. So every element of Hx can be written as an element of Hy :

$$hx = hh_3 y$$

$\forall h \in H$. So if Hx and Hy have any element in common, then every element of Hx is in Hy, and a similar argument shows the opposite. Therefore, if they have any one element in common, they have every element in common and are identical.

The right cosets of a group partition the group, or divide it into disjoint sets, and that each of these partitions contains the same number of elements.

Lagrange's Theorem: If G is a finite group, $H \leqslant G$, then $|H|$ divides $|G|$. So $m|H| = |G|$ for some $m \geq 1 \in N^+$

Proof. The right cosets of H in G partition G. Suppose there are m cosets of H in G. Each one is the size of the number of elements in H, or |H|.
G is just the sum of all the cosets: $G = h_1 G + h_2 G + \ldots + h_n G$, so its size is the sum of the sizes of all the cosets. So we can write $|G| = m|H|$.

Below is a list of some group generators and their sizes, all factors of the size of $\Re$:

Generators	Size	Factorization
U	4	2^2
U, RR	14400	$2^6 \cdot 3^2 \cdot 5^2$
U, R	73483200	$2^6 \cdot 3^8 \cdot 5^2$
RRLL, UUDD, FFBB	8	2^3
Rl, Ud, Fb	768	$2^8 \cdot 3$
RL, UD, FB	6144	$2^{11} \cdot 3$
FF, RR	12	$2 \cdot 3^2$
FF, RR, LL	96	$2^5 \cdot 3$
FF, BB, RR, LL, UU	663552	$2^{13} \cdot 3^4$
LLUU	6	$2 \cdot 3$
LLUU, RRUU	48	$2^4 \cdot 3$
LLUU, FFUU, RRUU	82944	$2^{10} \cdot 3^4$
LLUU, FFUU, RRUU, BBUU	331776	$2^{12} \cdot 3^4$
LUlu, RUru	486	$2 \cdot 3^5$

Table 2.4:

2.10 Cayley Graphs

The following properties describe a Cayley graph of a group G :

1. Each $g \in G$ is a vertex.

2. Each group generator $s \in S$ is assigned a color c_s.

3. For any $g \in G, s \in S$, the elements corresponding to g and gs are joined by a directed edge of color c_s.

The following is the Cayley graph for the subgroup generated by F :

Note 2.10.1. If two groups have the same Cayley graph, they have essentially the same structure and are called **isomorphic.**

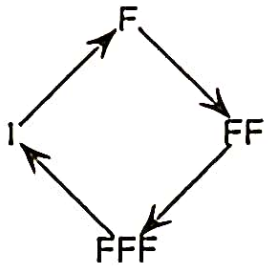


Figure 2.5: Cayley graph

Two isomorphic groups will have the same order and the same effect on the cube. For example, performing $FFRR$ has the same effect as rotating the cube so that the L face is now in front and then performing $RRBB$.

2.11 Macros

A macro is an action or a set of actions that you can run as many times as you want. We first define some properties of cube group elements and then use these properties to develop some **macros** or combinations of cube moves that will help us accomplish specific cubie rearrangements that will enable us to solve the cube.

2.12 Commutator

- If X and Y are two moves on a Rubik's cube, their commutator is the move $XYX^{-1}Y^{-1}$.
- $XYX^{-1}Y^{-1} = 1$ exactly when X and Y commute. (Because $XYX^{-1}Y^{-1} = (XY)(YX)^{-1}$ which equals to the identity when $(YX)^{-1}$ is the inverse of XY, i.e., when $YX = XY$.
- Commutators are a very useful tool in solving a Rubik's Cube.

Examples of Commutator

1. Flipping two edges
2. Rotating two corners
3. Cycling three corners
4. Cycling three edges

2.13 Conjugation

Let M be some macro that performs a cube operation, say a 3 - cycle of edge pieces. Then we say for some cube move P, PMP^{-1} is the conjugation of M by P.

An equivalence relation is any relation $\sim$ between elements that are:

- Reflexive: $x \sim x$
- Symmetric: If $x \sim y$, then $y \sim x$

- Transitive: If $x \sim y$ and $y \sim z$, then $x \sim z$

We will let the relation $\sim$ be conjugacy. So if for some $g \in G$,x $\sim$ y, then $gxg^{-1} = y$. Here we prove that conjugacy is an equivalence relation:

- Reflexive: $gxg^{-1} = x$ if $g = 1$, so $x \sim x$.
- Symmetric: If $x \sim y$, then $gxg^{-1} = y$, so multiplying g on the right and g^{-1} on the left gives $x = g^{-1}yg$.
- Transitive: If $x \sim y$ and $y \sim z$, then $y = gxg^{-1}$ and $z = hyh^{-1}$, so $z = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$, so $x \sim z$.

An **equivalence class** $c(x), x \in G$ is the set of all $y \in G : y \sim x$. We can partition G into disjoint equivalence classes, or conjugacy classes.

Two permutation elements of $\Re$ are conjugates if they have the same cycle structure. The following example makes this more clear.

In solving a cube, one straightforward approach is to solve it layer by layer. Once we get to the third layer, some of the edge pieces might be flipped the wrong way as in the following picture.

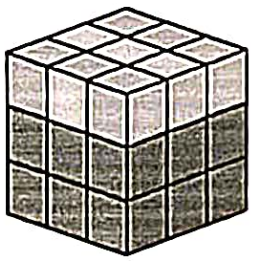


Figure 2.6:

We want to flip these pieces correctly, but leave the bottom two layers intact.

We can use conjugation to do so. Consider the move consisting of the commutator $g = RUru$. Applying g to the cube has the effect shown below (Fig 2.7).

It is seen that 7 cubes are affected, 2 of which are not in the top layer, but cubies in all the positions are affected by the macro so that the top layer cubies are rearranged.

Figure 2.7:

Now, take the conjugate of g by F to get the move $FRUruf$ (Fig. 2.8).

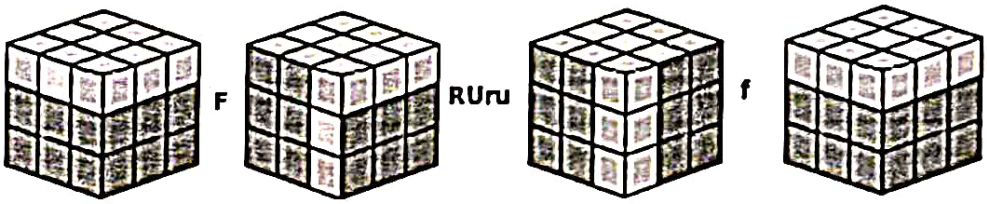


Figure 2.8:

Chapter 3

The Rubik's cube and the word problem

Definition 3.1. Given a list L of questions, a decision algorithm for L is a uniform set of unambiguous instructions which, when applied to any question in L gives the correct answer "yes" or "no" after a finite number of steps.

3.1 Background on free groups

Let $X = \{x_1, \ldots, x_n\}$ denote a set and X^{-1} a set disjoint from X whose elements we denote by $\{x_1^{-1}, \ldots, x_n^{-1}\}$. Assume that the map $x \longmapsto x^{-1}$ defines a bijection $X \to X^{-1}$. It will be convenient to let $x^1 = x, x_i^0 = 1$, where 1 is an element not belonging to $X \cup X^{-1}$ which we will call the identity element. A word on X is a sequence

$$w = (a_1, a_2, \ldots, a_N)$$

where $N > 0$ is some integer and each a_i belongs to

$$X \cup X^{-1} \cup \{1\}$$

The sequence of all 1's is called the empty word. The inverse of the word w is the word

$$w^{-1} = (a_N^{-1}, \ldots, a_1^{-1})$$

If $a_i = y_i^{e_i}$, where e_i is in $\{0, 1, -1\}$ and $y_i \in X$, then we shall write the word w as $w = y_1^{e_1} \ldots y_N^{e_N}$.

Example.3.1.1 Let $X = \{R, L, U, D, F, B\}$. The set of words on X are in a bijective correspondence with the set of sequences of basic moves you can make on the Rubik's cube.

We call a word $w = y_1^{e_1} \ldots y_N^{e_N}$ on X reduced if either w is empty or if the exponents e_i are non-zero and if there are no $x \in X$ with x, x^{-1} adjacent in w.

Definition.3.1.1. The free group $F_n = F_X$ on the generators $x_1, \ldots, x_n$ is the group of all reduced words on X.

3.1.1 Length

If, in the notation above, $w = y_1^{e_1} \ldots y_N^{e_N}$ is a reduced word (so $e_i \in \{0, 1, -1\}$) then we call N the length (or reduced length, to be more precise) of w.

If $G =< g_1, \ldots, g_k > \subset S_n$ is a finite permutation group generated by permutations $g_1, \ldots, g_k$ then we may still define the notion of length:

Definition.3.1.1.1. Suppose $g \in G$ is not the identity, where G is a permutation group as above. Then g may be written

$$g = y_1^{e_1} \dots y_N^{e_N}$$

where each $y_i \in \{g_1, \dots, g_k\}$ and where $e_i \in \{0, 1, -1\}$. The number N and the sets $\{y_1, \dots, y_N\}, \{e_1, \dots, e_N\}$ may not be unique for a given g but among all such possibilities there is at least one such that the value of N is minimum. We call this the length of g, denoted $\ell(g)$.

Let

$$P_G(t) = \sum_{g \in G} t^{\ell(g)}$$

This is called the Poincare polynomial of G.

The length of g is the distance in the Cayley graph between the vertex g and the vertex 1. The problem of determining the largest possible distance in the Cayley graph of the Rubik's cube group is known as "God's algorithm" and is currently unsolved.

Example.3.1.1.1. Let $G = S_n$ with generators $g_i = (i, i+1), i = 1, \dots, n-1$. The Poincaré polynomial is known:

$$\Pi_{k=1}^{n} \frac{t^{k+1} - 1}{t - 1}$$

3.1.2 Trees

We may represent the free group graphically as follows. We define the Cayley graph of F_n inductively:

- Draw a vertex for each element of $X \cup X^{-1}$ (these are the vertices, V_1 say,

for the words of length 1),

- Suppose we are given that you have already drawn all the vertices for the words of length $k-1, V_{k-1}$ let's call them. For each $x \in X \cup X^{-1}$ and each $v \in V_{k-1}$, draw a vertex for each word of length k obtained by multiplying v by x on the right, $v * x$, and connect v and $v * x$ by an edge.

There are infinitely many vertices, each of which has degree $|X \cup X^{-1}|$. Moreover, this graph has no circuits or loops (i.e., no path of edges crosses back over onto itself). Such a graph is called a tree.

Example.1.2.1. Let $X = \{R, L, U, D, F, B\}$. The elements of the free group F_X correspond to the mechanically different sequences of basic moves you can make on the Rubik's cube. Of course, different sequences of moves may yield the same position of the Rubik's cube (e.g., R^4 and 1 are the same position but sequence of moves used to attain them are distinct).

There are infinitely many vertices of the Cayley graph of F_X, each of which corresponds to a mechanically distinct move of the Rubik's cube.

3.2 The word problem

There is a was to list all the elements of F_n, called the lexicographic ordering. Give an algorithm for determining if a word $w \in F_n$ occurs before a word w', in which case we write $w < w'$. For example, distingish between the the identity 1 and the "non-reduced" word $x_1 * x_1^{-1}$.

The first element in this lexicographically ordered list is the word 1, the next $2n$ words are the words

$$x_1 < x_1^{-1} < \ldots < x_n < x_n^{-1}$$

In general, we define $y_1..y_M < z_1 \ldots z_N$ if either (a) $M < N$ or (b) $M = N$ and $y_1 < z_1$ or $y_1 = z_1$ and $y_2 < z_2$ or $y_1 = z_1$ and $y_2 = z_2$ and $y_3 < z_3$ or ....

List all the elements of F_n as

$$F_n = \{w_1, w_2, \ldots\}$$

so $w_1 = 1, w_2 = x_1, \ldots$ Let G be a subgroup of F_n or a permutation group $G =< g_1, \ldots, g_n >$. If G is a permutation group then we regard a word w_k as an element of G by substituting g_i for each $x_i, 1 \leq i \leq n$.

Theorem.3.2.1.. A decision algorithm for the word problem for the Rubik's cube group with generators R, L, U, D, F, B is the same as an algorithm for solving the Rubik's cube.

3.3 Generators, relations, and Plutonian robots

Here's a hypothetical situation: You and a friend each have a robot on the planet Pluto with a scrambled Rubik's cube. You and your friend also have duplicate cubes, scrambled the same way as your robots. (We will call the robots R^2D^2 and R^2B^2 if you don't mind!) These robots have manual dexterity but no pre-programming on how to solve the cube. Furthermore, assume it is very expensive to program different moves, so you want to teach the robot the smallest number of separate moves that you can. On the other hand, the moves need not be basic moves (U,R,..) since it we will assume it costs roughly the same to teach the robot

the move R as the move $R * U^2 * R^{-1}$, for example. Your solution will be a "word" in these taught moves. Again, to minimize the cost of transmission, you want the "word" to be absolutely as short as possible. A prize of 1 million dollars has been set up to the first of you who can get their robot to solve its cube.

In other words, we want to solve the word problem for the cube and we want to do it as efficiently as possible. Suppose we know we need n generators and we know that this is the smallest number. How do we make a "word" as short as possible? To make a word in these generators as small as possible, we must know all the "relations" between these generators so we can, if necessary, substitute them into the word and perform some cancelation. This is what this section is about.

Let X be a finite set, say $n = |X|$. Let Y be a set of reduced words on X. Let R be the smallest normal subgroup of F_n containing Y. Since R is normal, the quotient F_n/R is a group.

Definition.3.3.1. Let G be a group. We say that G has generators X and relations Y if G is isomorphic to F_n/R. A collection of generators and relations defining a group is called a presentation of the group.

As a matter of notation, an element $r \in R$ is written as an equation $r = 1$ in G.

Remark.3.3.1. Gives a topological interpretation of R as "the fundamental group of the Cayley graph of G with respect to X ".

Example.3.3.1 The cyclic group of order $3, C_3$, has one generator x and one relation $x^3 = 1$, so

$$X = \{x\}, \quad R = \left\{ (x^3)^k \mid k \in \mathbb{Z} \right\} \subset F_1 = \left\{ x^k \mid k \in \mathbb{Z} \right\}$$

Here the cosets of F_1/R are R, xR, x^2R. The set of these three cosets is closed under multiplication. For example, $(xR)(x^2R) = x(Rx^2)R = xx^2RR = x^3R = R$, so the inverse of the element xR is x^2R.

More generally, C_n has presentation

$$C_n = \{x \mid x^n = 1\}.$$

3.4 The presentation problem

The following problem is unsolved:

Problem: Let G be the Rubik's cube group. Find a set of generators and relations for G of minimal cardinality (i.e., $|X| + |Y|$ is of minimal cardinality).

Problem.3.4.1 : Find

(a) a set of generators for G of minimal cardinality,

(b) a set of relations for G of minimal cardinality,

(c) an expression for each such generator as a word in the basic moves R, L, U, D, F, B.

The part (a) is known: there are 2 elements which generate G. Part (b) is not known (though Dan Hoey's post of Dec 17, 1995 to the cube-lover's list may describe the best known results ; he suggests that G has a set X of 5 generators and a set Y of 44 relations such that the total length of all the reduced words in Y is 605).

3.4.1. A presentation for $C_m^n > \triangleleft S_{n+1}$

We begin an assault on the problem of D. Singmaster mentioned above. This section was written with Dennis Spellman.

We can identify the $C_m^n > \triangleleft S_{n+1}$ with the group of $(n+1) \times (n+1)$ invertible monomial matrices g with coefficients in C_m having the following condition on the determinant: if we write $g = p \cdot d$, where p is a permutation matrix and d is a diagonal matrix then $\det(d) = 1$ (this determinant 1 condition is a condition corresponding to the "conservation of twists" for the moves of the Rubik's cube).

We may identify C_m^n with the subgroup

$$\{(x_1, \ldots, x_{n+1}) \mid x_1 x_2 \ldots x_{n+1} = 1, x_i \in C_m\}$$

and $C_m^n > \triangleleft S_{n+1}$ as a subgroup of the wreath product $S_{n+1} wr C_m$.

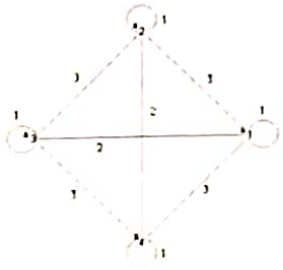
Consider $G = C_m^{n+1} > \triangleleft S_{n+1}$. The group S_{n+1} has presentation

$$S_{n+1} =< a_1, \ldots, a_n \mid (a_i a_j)^{m_{ij}} = 1, \forall 1 \leq i, j \leq n >$$

where

$$m_{ij} = \begin{cases} 3, & j = i \pm 1 \\ 2, & |i - j| > 1 \\ 1, & i = j \end{cases}$$

The following diagram may help to visualize the exponents m_{ij} in the case $n = 4$:



As a group of $(n+1) \times (n+1)$ monomial matrices, we identify a_i with the permutation matrix,

$$s_i = \begin{pmatrix} 1 & 0 & & \cdots & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & 1 \\ & & & & \iddots & \\ 0 & \cdots & & & 0 & 1 \end{pmatrix}$$

If I is the $(n+1) \times (n+1)$ identity matrix and if E_{ij} denotes the matrix which is 0 in every entry except the ij entry, which is 1 , then

$$s_i = I - E_{ii} - E_{i+1,i+1} + E_{i,i+1} + E_{i+1,i}.$$

The group C_m has presentation

$$C_m = < h \mid h^m = 1 > .$$

The group C_m^n has presentation

$$C_m^n = < h_1, \ldots, h_n \mid h_i^m = 1, h_i h_j = h_j h_i, \forall 1 \leq i, j \leq n+1 >$$

We identify C_m^n with the Cartesian product

$$\{(h_1(x_1), h_2(x_2), \ldots, h_n(x_n)) \mid x_i \in C_m\}$$

where $h_i(t)$ is the diagonal matrix

$$h_i(t) = I - E_{ii} - E_{i+1,i+1} + tE_{i,i} + t^{-1}E_{i+1,i+1}.$$

There are the following identities between the s_i and the $h_j(t)$:

$$s_i h_j(t) s_i^{-1} = h_j(t), \quad |i-j| > 1$$

$$s_i h_i(t) s_i^{-1} = h_i(t)^{-1}$$

$$s_{i\pm1} h_j(t) s_{i\pm1}^{-1} = h_i(t) h_{i\pm1}(t).$$

Theorem.3.4.1

$$(a_i a_j)^{m_{ij}} = 1,$$

$$\forall 1 \leq i, j \leq n,$$

$$h_i^m = 1, h_i h_j = h_j h_i, \forall 1 \leq i, j \leq n$$

$$a_i h_j a_i^{-1} = h_j, \quad |i-j| > 1,$$

$$a_i h_i a_i^{-1} = h_i^{-1}, \ldots, a_n, h_1, \ldots, h_n \mid$$

$$a_{i\pm1} h_j a_{i\pm1}^{-1} = h_i h_{i\pm1} >$$

Remark.3.4.1. The above result was proven before it was noticed that essentially the same presentation may be found in the paper by Davies and Morris (where the group $C_m^n > \lhd S_{n+1}$ is called a generalized symmetric group).

Chapter 4

Methods of solving the Cube

4.1 The Screwdriver Method

It involves turning one face 45 degrees, prying out the edge piece sticking out, and disassembling the cube using a screwdriver.

4.2 The Bottom-up method

This is one of the most intuitive, but probably one of the slowest, ways to solve the cube. It averages about 100 moves per solution.

1st Layer

This first layer must be done by inspection. There is usually no set algorithm to follow. It is helpful to focus on getting a cross first with the edge pieces correctly in place and then solving the corner one by one.

2nd Layer

Now rotate the bottom (solved) layer so that its edges on the other faces are paired with the correct centerpieces. The cube should look as follows:

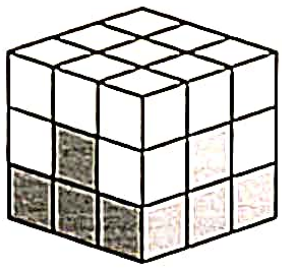


Figure 3.1:

For this layer we only have to solve the four middle layer edge pieces. If an edge piece is in the top layer, use the following macros (Fig 3.2) and (Fig 3.3).

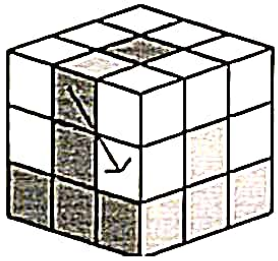


Figure 3.2: URurFrfR

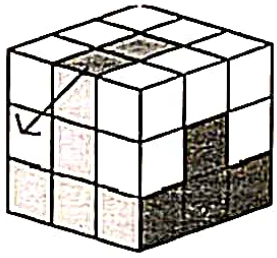


Figure 3.3: ulULfLFl

If an edge piece is not in the top layer, but is not oriented correctly, use the following to put the piece in the top layer and then proceed as above (Fig 3.4). The second layer is solved now.

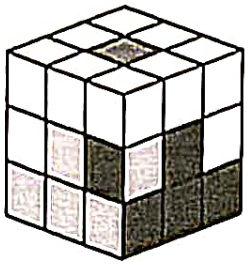


Figure 3.4: URurFrfR

3rd Layer

We will do this layer in 3 steps:

1. Flip the edges to form a cross on the top. Use this macro to flip a top layer edge correctly (Fig 3.5).

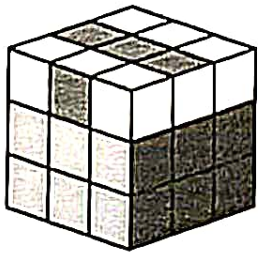


Figure 3.5: FRUrufU

Repeat until all the edge pieces form a cross on the top (Fig 3.6).

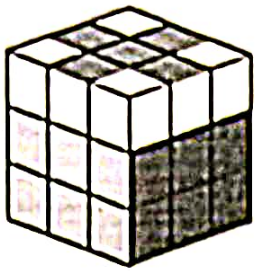


Figure 3.6:

2. Position the top layer edges correctly. Now position the top layer so that one of the edges is solved. If all the edges are solved, move on to the next step. If not, use the following algorithms to permute the edges correctly (Fig 3.7 & Fig 3.8).

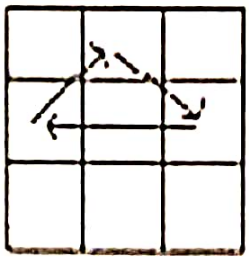


Figure 3.7: RU^2 ruRur

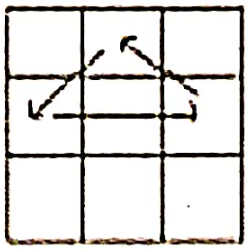


Figure 3.8: $RUrURU^2r$

If none of these work, apply one of them until a position is got where one of these will work, then proceed.

3. Flip the top layer corners: For each corner that does not have the correct color on the top layer, position it at UBR and perform $RDrd$ repeatedly until it is oriented with the correct color on top. Then, without rotating the cube, position the next unsolved corner at UBR and repeat the process. The bottom two layers will appear to be a mess, but they will be correct once all four corners are facing the correct direction (Fig 3.9).

4. Position the top layer corners correctly: Now the top layer should have all the same color faces, but the corners might not be oriented correctly. Position one corner correctly and then determine whether the others are solved, need to be rotated clockwise, or need to be rotated counterclockwise, and then apply the following (let $x = rD^2R$):

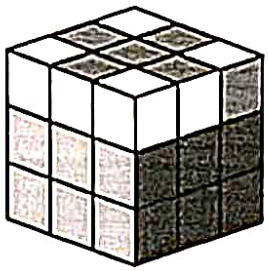


Figure 3.9:

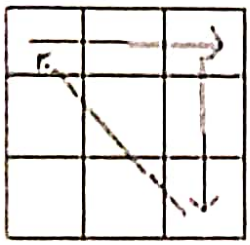


Figure 3.10: xU^2 xuxux

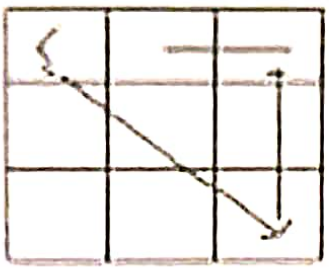


Figure 3.11: $xUxUxU^2x$

4.3 Other Methods

The other methods to solve the cube are :

1. CFOP: Cross, First two layers, Orient the last layer, and Permute the last layer. Invented in the 1980s by Jessica Fridrich.

2. Petrus Method: Solve a 2 by 2 by 2 block first, expand this 2 by 2 by 3 , fix the improperly oriented edges on the outside layer, and then solve the rest.

Conclusion

A Rubik's Cube is an interesting puzzle invented by 'Erno Rubik' which has 43 quintillion possible configurations. But with the use of certain algorithms, it can be solved easily. The math behind Rubik's Cube is a piece of abstract algebra called group theory, which emerged from studying symmetry. Group theory includes not just the symmetry of shapes but also less visible forms of symmetry in, say, the solutions to an equation and four-dimensional spacetime. This paper explored some of the group theory applications to the Rubik's cube and constructed the Rubik's Cube Group. The Rubik's Cube Group was shown to be $G = \langle R, B, L, U, F, D \rangle$, which is a subgroup of S_{54}. The Fridrich method or the CFOP method (cross, F2L, OLL, PLL) is a fast method for solving the Rubik's Cube created by Jessica Fridrich. It consists of four steps: Cross, F2L (First Two Layers), OLL(Orient Last Layer), and PLL (Permute Last Layer). The scope of this paper was restricted to the 3×3 Rubik's Cube Group. Erno Rubik took almost three months to solve a cube but by the introduction of algorithms, the fastest solver can solve the cube within seven seconds or less. In the first chapter, we have discussed the basic definitions related to our field of study. In the second chapter, we have moved deep into the concept of the Rubik's Cube, In the third chapter we have discussed about the Rubik's cube and word problems, and the fourth chapter we have studied dif-

ferent methods of solving the cube. With focus and constant practice, anyone can get faster at solving a Rubik's cube!

References

1 Jaslyn Lek. The Mathematics of the Rubik's Cube, Introduction to Group Theory and Permutation Puzzles, March 17, 2009.

2 Michael Hutchings, The Mathematics of Rubik's Cube, January 30, 2011.

3 Prof. S. G. Sanmukh, Mr. Somayya. S. Avadut. Rubik's Cube Algorithm.

4 Raymond Tran. A Mathematical Approach to Solving Rubik's cube, UBC Math308 - Fall 2005.