

# Rubiks Cube Project

ep15193

October 2017



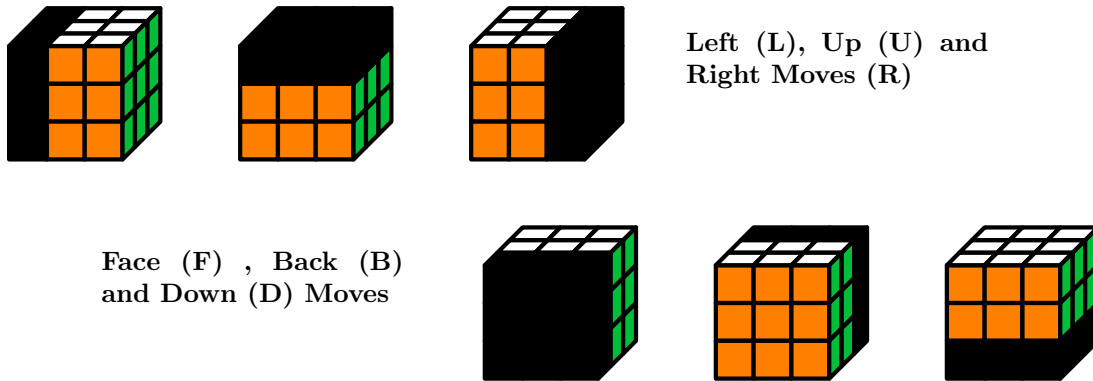
University of  
**BRISTOL**

basically a dissertation

# Contents

Notes . . . . .	3
<b>Introduction</b>	<b>3</b>
History on the cube . . . . .	3
Possible and non possible moves . . . . .	4
Goal of the project . . . . .	4
Important Theorems and Lemmas . . . . .	4
Groups, Subgroups . . . . .	4
Example . . . . .	5
Automorphisms . . . . .	5
<b>Alternating and Symmetric Groups</b>	<b>6</b>
<b>Context on Cube</b>	<b>10</b>
Generating and Minimally generating subgroups . . . . .	10
Generators . . . . .	10
<b>Possible and Non Possible Configurations</b>	<b>13</b>
<b>Applications</b>	<b>20</b>
Normal Subgroup . . . . .	20
Semi-Direct Product . . . . .	20
Wreath Products . . . . .	20
Illegal Rubiks Cube Group . . . . .	20
Legal Rubiks Cube Group . . . . .	21
<b>Possible Extension- CRAN cubing package</b>	<b>22</b>
Thistlethwaite's Algorithm . . . . .	25
<b>References</b>	<b>26</b>

The cube is made up out of 27 small cubes , referred to as cubies. These include the 8 corner cubies , 12 edge cubies and the 6 center ones with one non-visible 'cube' in the middle.



Above shows the 6 basic moves of the cube, to which the black cubies are transformed by rotating the specific face 90 degrees clockwise. When applying one of these moves it is necessary to reference how to describe the change of the cubie. Fixing the cubies in the start configuration allows to reference cubicles .....&&&&&&&&

## Notes

Homomorphism to identity - we know there is one because there is a solved configuration.

By FHT we know  $G_{corner}/Z_3 \leq S_8$  the kernel is a normal subgroup of a group homomorphism , which is G corner.

Can check individual moves correspond to 0 mod 3 , check symmetric groups on moves e.g. LR RLUDFB

## Introduction

### History on the cube

(Limited, 2017) The cube was first created by a Hungarian Professor named Erno Rubik. The original version is one which mimics the cube seen today including the coloured stickers. To him it wasn't meant to be a hobby or game like element, instead it was created to aid him in explaining three dimensional geometry. Although being the creator ,he found as he mixed up the cube and the stickers became jumbled he was unable to solve it. *It was a code I myself had invented!" he wrote. "Yet I could not read it."* Thus creating the phenomenon seen today, with a staggering 400 million sold and 1 in 7 people believed to have played with the cube. After this amount of time the cube has still not fallen out of popularity.With 'SpeedCube' competitions still rife the world record

Singmasters (Singmaster, 1981) notation states that there are 6 basic moves of the rubiks cube (RLUFDB) which will be referenced throughout this project.

The cube has 8 corner cubies have 3 faces while the 12 edge cubies have 2 faces leaving the 6 center cubies with a singular face. When applying one of these basic moves to the cube it's impossible for these center cubies to stray from the cubicle in which they live in. So applying probability to the scenario, should allow to calculate the total number of configurations. There is a choice of  $8!$  positions for the corner cubies, and as there's 3 faces there are  $3^8$  possible orientations. Similarly with the 12 edge cubies, combining these results give a total of  $2^{12} * 3^8 * 8! * 12! \approx 519$  quintillion configurations. However what isn't known yet is which of these are actually possible from a set of permutations from the starting configuration.

This gives us motivation to see which of these configurations are not valid, why they're not valid.....&&&&&&&&

A group  $G$  is defined as a set with a binary operation  $*$  such that  $, * : G \times G \rightarrow G$ . Which follows these properties.

- A homomorphism is a function  $\phi$  from two groups  $G$  and  $H$ , such that  $\phi$  preserves the group operation

4

### Example

Group of multiplication  $\in \mathbb{Z}$ .

The group definition is very useful when understanding following theorems and lemmas about the cube and can be applied directly below.

The group of the Rubiks Cube  $(G, *)$  can be represented by the cube permutations, composed of the 6 basic moves of the cube listed previously. This group will be a subset of size to the total configurations calculated in the Introduction as here the group actions (which can create a configuration) will be defined explicitly.

EXPAND PROOF ,M be a set of moves

- G is closed under  $*$ ,
- e is the empty move , do nothing
- if there is a move M then inverse is just reversing what you did
- Associativity is more complex proof &&&&&&

### Automorphisms

This is just any isomorphism which is a mapping from one object to itself. The set of all of these automorphisms in an object form the automorphism group.

## Alternating and Symmetric Groups

Let  $X$  be a set and let  $S(X)$  be the symmetric group on  $X$ ; the elements of  $S(X)$  are the permutations of  $X$  (i.e. bijections  $X \rightarrow X$ ) and the group operation is composition of maps. In contrast an Alternating group  $A(X)$  only contains the permutations to which are just even cycles, as opposed to the symmetric group above containing even and odd cycles. For notation purposes these two groups will be defined as  $A_n$  and  $S_n$ .

A useful map to consider is an operation called a group homomorphism between two groups defined by the following properties:

$\phi : G \rightarrow H$  is a homomorphism if :

*The map is a well – defined mapping*

$$\phi(ab) = \phi(a) * \phi(b) \quad \forall a, b \in G$$

$$\text{im}(\phi) = \{\phi(a) | a \in G\}$$

$$\ker(\phi) = \{a \in G | \phi(a) = e'\}$$

In our case we can define a function as below which will map the elements of  $S_n$  to either 1 or -1 in the cases outlined in the definition below.

$$\phi : S_n \rightarrow \{-1, 1\} \quad \phi(x) = \begin{cases} 1, & \text{if } x \text{ is an even number of transpositions.} \\ -1, & \text{if } x \text{ is an odd number of transpositions.} \end{cases} \quad (2)$$

When  $x \in \phi(x)$  equals 1, it means it can be expressed as an even number of transpositions. Transpositions are defined as the 2 cycle permutations, but to show the well-defined property of this map we need to first show all permutations in  $S_n$  can be written as a product of transpositions. This can be shown by the following inductive argument. The base case for  $S_2$  is trivial. Suppose any permutation of  $n$  takes less than  $n$  transpositions. Consider a permutation  $w$  of length  $n+1$  (transpositions). Using the base case we can perform one transposition to swap the  $n+1^{st}$  element in the correct place. Thus by the inductive hypothesis we have less than  $n$  transpositions for the remaining  $n$  elements, making the total less than  $n+1$  transpositions. Now this is known the map can be shown to be a homomorphism by the following.

*Proof.*

Our map can easily be verified to satisfy the conditions above. It is well defined, it can be expressed as some product of transpositions by the proof above.

Take two elements  $\sigma, \tau \in S_n$ . The goal is to show  $S_{\tau\sigma} = S_\tau * S_\sigma$

Either of these can be written like so  $\sigma = \alpha_1 \dots \alpha_a, \tau = \beta_1 \dots \beta_b$ , with some integers  $a$  and  $b$  factorizations of  $\alpha$  and  $\beta$  as a product of transpositions.

$\sigma\tau = \alpha_1 \dots \alpha_a \beta_1 \dots \beta_b$  now expresses  $\sigma\tau$  as a product of  $a+b$  transpositions.

$$\phi(\sigma\tau) = (-1)^{a+b} = (-1)^a (-1)^b = \phi(\sigma)\phi(\tau)$$

thus conditions of homomorphisms are satisfied. □

As the map is known to be a homomorphism the kernel  $\ker(\phi)$  is of the form  $\{a \in G \mid \phi(a) = e'\}$  where  $e'$  is the identity element of the set  $\{-1, 1\}$ . For this case as the identity of this set cannot be 0 as a norm for groups such as  $(\mathbb{Z}, +), (\mathbb{N}, +)$  as the 0 element does not exist thus shall be defined at the elements of even cycles (odd transpositions). So we have  $A_n \subset \ker(\phi)$  but also it is the entire kernel itself so  $A_n = \ker(\phi)$ , if it wasn't then for some  $S_n \notin A_n \in \ker(\phi)$ . However this cannot be the case as only even cycles are mapped to -1, and any even cycles in  $S_n$  are in  $A_n$  by definition. Taking into consideration the Group Homomorphism Theorem, or alternatively the First Isomorphism Theorem

**Theorem 0.1** (Group Homomorphism Theorem).  $G/\ker(\phi) \cong \text{im}(\phi)$

Showing that the group  $G$  / by the kernel is isomorphic to the image of the group. Being isomorphic means there exists a homomorphism between the two groups which is also injective (one to one). Substituting the values above defined for the kernel and the image of the group, it can be concluded that,

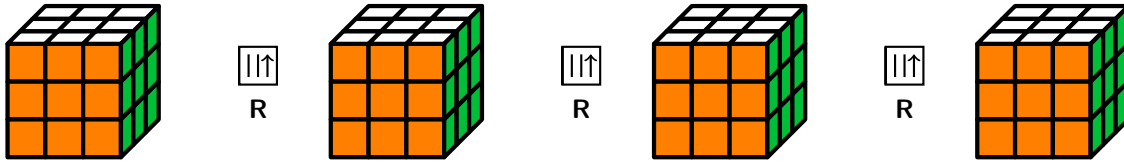
$$S_n/A_n \cong \mathbb{Z}_2 \quad (3)$$

The cyclic group  $\mathbb{Z}_2$  is placed at the end as it is equivalent to the set of  $\{1, -1\}$  with just two elements,  $x$  and the identity (as  $x$  is the 1 and the identity has already been defined to be -1).

From the Group Homomorphism Theorem there is now a new collection called a quotient group, but to understand what a quotient group is to groups one must first consider the left and right cosets formed by each corresponding group. With  $G$  a group and  $H$  a subgroup of  $G$  the left and right cosets are as follows:

- $gH = \{gh \mid h \in H\}$  is the left coset
- $Hg = \{hg \mid h \in H\}$  is the right coset

The subgroup  $H$  is just the smallest group contained in  $G$  which generates all the elements of  $H$ . Taking  $H = \{R\}$  (the right turn) as an example,  $H$  is now the subgroup of  $\mathcal{G}_{RC}$  generated by all right turns as shown.



This is one instance of a right coset purely by definition on the original group  $\mathcal{G}_{RC}$ . It is such that whatever the size of the subgroup  $H$  it is identical to size of the coset. This is by construction as there is one element in the coset for each element in the subgroup. It can also be said that any two coset from a subgroup  $H$  constructing from the group  $G$ , must be either distinct or the same. So any subgroup must have disjoint cosets, making them unique in definition. This can be shown by a simple proof by contradiction:

*Proof.*

Suppose there were two right cosets  $Hx$  and  $Hy$  which share elements.

$h_1x = h_2y$  for some  $h_1, h_2 \in H$

taking inverses  $x = h_1^{-1}h_2y$  ,  $h_3 = h_1^{-1}h_2$

thus  $x = h_3y$  and  $hx = hh_3y$

so every element of  $Hx$  can be written as one of  $Hy$

so every element of  $Hx$  is in  $Hy$ , thus  $Hx = Hy$  □

These such right cosets will partition the rubiks cube group into equal sized disjoint sets. As the kernel of  $\mathcal{G}_{RC}$  is a group itself, the number of distinct cosets is the size of the quotient  $|G|/|ker(\phi)$ . This is by Lagrange's Theorem.

**Theorem 0.2** (Lagrange's Theorem). *For  $H$  a subgroup of a group  $G$  , the size of  $H$  must be a divisor of the size of  $G$ . So  $x|H| = |G|$  for some  $x \geq 1$*

So now there is the quotient group  $S_n/A_n$  is isomorphic to  $\mathbb{Z}_2$  and of order dividing the rubiks cube group  $\mathcal{G}_{RC}$  by Lagrange, now whats left is to show is that the map  $\phi : S_n/A_n \rightarrow \{1, -1\}$  preserves an homomorphism as above. As the alternating group has been defined as the kernel above , the group operation (multiplication) will hold in a similar way to the  $\phi : S_n \rightarrow \{1, -1\}$  map. There are 4 possible occurrences of multiplication in this map defined below.

$$x \text{ is even, } y \text{ is even} \quad \phi(xy) = \phi(x)\phi(y) = 1 * 1 = 1 \quad (4)$$

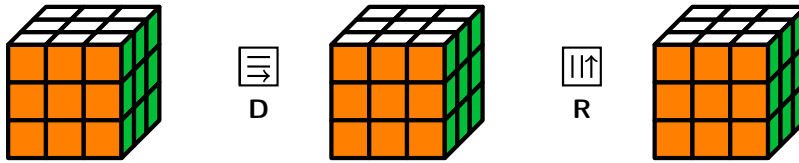
$$x \text{ is even, } y \text{ is odd} \quad \phi(xy) = \phi(x)\phi(y) = 1 * (-1) = -1 \quad (5)$$

$$x \text{ is odd, } y \text{ is even} \quad \phi(xy) = \phi(x)\phi(y) = (-1) * 1 = -1 \quad (6)$$

$$x \text{ is odd, } y \text{ is odd} \quad \phi(xy) = \phi(x)\phi(y) = (-1) * (-1) = 1 \quad (7)$$

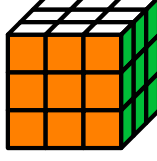
Note: By  $x$  is even ,  $y$  is odd , it means for  $x$  to be defined as even number of transpositions ,  $y$  to be odd number of transpositions. So homomorphic property of multiplication holds, thus map must be homomorphic.

While presently this may not seem that important this conclusion will be paramount in defining the analysis of the cube. This will be referenced later on in the project after valid configurations have been defined. Now this theory can be related to the example of the 3 by 3 cube. Consider the move  $DR^{-1}$  on the start configuration of the cube. **USE VIDEO EXPLANATION**



Only considering the corner cubies for now, labeling them appropriately will allow for the moves to be expressed as a combination of disjoint cycles. The group considered when making these permutations is the group of all corner cubies  $Z_3^8$ . The labeling of the cube is as such **\*\*\*INSERT LABELLING\*\*\***





$$D(\theta) = (1)(2)(3)(4)(5\ 6\ 7\ 8) \quad R^{-1}(\theta) = (1\ 7\ 8\ 4)(2)(3)(5)(6) \quad (8)$$

Are the cycles of the Down and Right inverse moves respectively which can be combined to obtain.

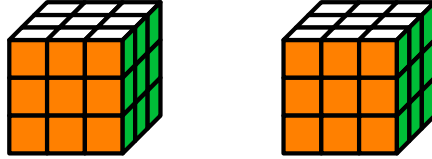
$$DR^{-1}(\theta) = (1\ 8\ 4)(5\ 6\ 7) \quad (9)$$

Now there is a cycle which alternates the position of the 6 cubies listed above. However this doesn't really achieve anything when looking to solve the cube, as far as the user is concerned this is just any random move  $M \in G$ . Aiming for a set of moves which oriented 2 cubies for instance would be far more useful in proving properties of the corner cubies and it's corresponding group  $Z_3^8$ . Taking the inverse of the move above,  $D^{-1}R$ , one obtains a similar disjoint cycle set of ,

$$D^{-1}R(\theta) = (1\ 7)(5\ 8) \quad (10)$$

These cycles are in fact isomorphic , which there is a combination which actually achieves the aim. Through inspection applying the moves together the combination is as follows

$$(DR^{-1}D^{-1}R)^2U^{-1}(DR^{-1}D^{-1}R)^4U \quad (11)$$



But this inspection doesn't seem very trivial and leaves the question why is this move above like so. For this explanation it's useful to turn to commutators from Group Theory.

*The commutator of two elements , g and h of a group G , is the element :  $ghg^{-1}h^{-1}$  (12)*

For the cube this can be translated by setting g,h to be a specific set of moves. So really what's done above is to find the commutator which orients the two corner cubies by using the definition of a commutator. Where instead of considering disjoint cycles , defining g and h like so

$$g = R^{-1}DRD^{-1}R^{-1}DR \quad h = U^{-1} \quad (13)$$

and applying the commutator algorithm  $(ghg^{-1}h^{-1})$  gives the set of moves to orient two corner cubies again. The importance of these commutators is high as it allows the user to gain intuition into actually solving the cube rather than just following a set algorithm. This also becomes particularly useful when the cube is a few moves off the start configuration and say the user needs to permute two corner cubies, now with the knowledge of the correct group commutator this can be achieved.

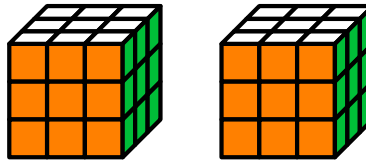
## Context on Cube

### Generating and Minimally generating subgroups

#### Generators

Let  $G$  be a group, a subset  $S \subseteq G$  is a generating set of  $G$  if  $G = \langle S \rangle$ . In other words every element of  $G$  can be written as a finite product (under group operation) of elements of  $S$ . These elements are called generators of  $G$ . Taking the group  $G$  to be composed of the 6 basic moves  $G = \{F, L, R, U, D, B\}$ , such that any cube permutation can be made, allows a comparison to be made of what a generator means to this specific example. For example taking  $S = \{R\}$  gives the subgroup which obtains all possible cube permutations obtained by rotating the right face  $\{R, R^2, R^3, R^4\}$ . As the order of a group is defined as either the least  $n \in \mathbb{N}$  such that  $g^n = e$  (where  $g$  is a member of the group), or alternatively the size of the subgroup it generates, the order for  $S$  will be 4. Note it stops at  $R^4$  as the group is cyclic\*, so  $R^5 = R$ . \*by cyclic it just means to say that there exists an element which creates a generating set.

In group theory many groups share the property of being Abelian, which means for a group  $G$  if  $\forall x, y \in G, x * y = y * x$ . One example could be  $(\mathbb{Z}, +)$  the group of the integers on addition, for any integer  $x, y$  this will hold ( $3+4 = 4+3$ ) as the integers are commutative and associative in definition. However applying this to the rubiks cube group this will not hold, showing us the order in which the moves are applied does in fact matter. This is shown by a simple case of the move  $M = \{L, R2, D\}$  below



Where, from the starting configuration, the left hand cube has been applied the sequence  $L, R2, D$  and the right hand cube  $R2, D, L$ . Visually one can see they are obviously not equal, thus breaking the condition of what it means to be abelian. This is because these moves share common cubies, a move consisting of opposite faces alone such as  $R, L$  would hold commutativity ( $RL=LR$ ) however for the whole cube this can't be said. So clearly some elements of the group commute while others do not.

The set of elements to which the generators are made from is defined as the generating set. These generators are a useful way for defining groups, however for large groups such as the rubiks cube it can become difficult to gain information due to the sheer enormity of possible generators. When talking about these commuting elements it is often useful to mention orbits and their stabilisers.

Given the definition of an orbit from Group Theory,

*if  $G$  acts on a set  $A$ , then the orbit of  $a \in A$  (under this action) is the set  $\{a * g : g \in G\}$*

*The stabiliser of an orbit is  $\{g \in G | g * x = x\}$  the set of all elements that fix  $x$*  (14)

From the definition the orbit is just the subset of  $A$  which can be moved by any move from  $G$ , with  $A$  being the total number of configurations of the cube. As said above the center cubies always stay in the 6 center positions hence will always be in the same orbit. This applies to the

corner and edge cubies as well (relative to corner and edge positions). From properties of an orbit, it must be either disjoint or the same (this can be shown from a single contrapositive argument). So one could consider 3 separate orbits within the Cube where,

$$A = A_x \cup A_e \cup A_c \cup A_e \quad (15)$$

$A_x$  are the center pieces,  $A_e$  edge pieces and  $A_c$  the corner pieces. We know any of these respective cubies will stay under their respective positions from a move  $G$ , but what isn't so is trivial is when considering the whole set of the cubies. Moreover prove how any group action from the Rubiks Group  $\mathcal{G}_R$  preserves any resulting configuration will be in the same orbit. (, ?) An example of when the wouldn't apply is any illegal configuration of the cube (e.g. from pulling pieces out, switching stickers etc.) ,defining the difference into what is and isn't a valid configuration is key in proving the statement about same orbits above. This will be referenced later in the paper. Orbits aswell as describing how points, or in the case described, cubies move can also be used to compute stabilisers. These can be the subgroups of elements which fix one or more points, which can be very useful in solving the cube in a step by step solution.(Wolfram, 2018)

Suppose there was an algorithm which took a given scrambled state to the starting configuration. Where in this algorithm one piece has been permuted correctly, call it  $G_1$ , where the rest of the cube remains to be solved. These subsequent permutations will aim to put their respective pieces in the correct place (and orientation) without disturbing the previous permutation.

This algorithm is called a stabiliser chain where the first permutation fixing the first piece of the cube,  $G_1$  shall be defined as the stabiliser of the chain.  $G > G_1 > G_2 > \dots > G_n = I$ , where  $I$  is the identity (starting configuration). Each of these  $G_i$ 's should contain a set of moves which solves the  $i$ 'th piece, therefore one of the move sequences for that  $G_i$  will be in  $G_{i+1}$ , a permutation in  $G_i$  will always lie in  $G_{i+1}$ . In other terms with a list of a move  $a_{i1}, a_{i2}, a_{i3}, \dots$  every  $b \in G_i \in a_{ik}G_{i+1}$  for some  $k$ . So  $G_i$  is made up entirely of the set of all cosets  $a_{i1}G_{i+1}, a_{i2}G_{i+1}, a_{i3}G_{i+1}, \dots$  for every  $k$ . There now exists a way to find the generators for  $G_{i+1}$  a specific sequence solving the  $i+1$ 'th piece, that given the generators of  $G_i$  and the list of move sequences  $a_{ik}$  (or coset representatives), the new stabiliser chain can be built.(Jaap, 1981)

The rubiks cube group  $\mathbb{G}_{RC}$  if to be implemented by a computer using each individual configuration, which is  $(8! * 3^8 * 12! * 2^{12}/3 * 2 * 2) \approx 4.3 * 10^{19}$ , becomes computationally inefficient to try and store each sequence for each configuration. The aim of implementing this algorithm however is to identify the groups composition structure by using subgroups to factorise the problem down, to solve the cube from a given state. The algorithm in question the Schreier Sims Algorithm, is given motivation from the Schreier Lemma on subgroups.

**Lemma 1** (Schreier Lemma on Subgroups). *Let  $G$  be a group with a set of generators  $S$ . Let  $H$  be a subgroup of  $G$ , and let  $A$  be the set of coset representatives of  $H \in G$ . For any  $g \in G$ , let  $g$  denote the element of  $A$  that represents the coset  $gH$ .*

*Then  $H$  is generated from the set  $\{(sa)^{-1}(sa) | a \in R, s \in S\}$ .*

*Proof.* Take any  $h \in H(\in G)$ ,  $h = s_1 s_2 \dots s_k$  for some sequence of generators  $s_i \in S$ .

Let  $t_i = s_{i+1} \dots s_k$  be the coset representative for the  $s$  sequence

, this is such that  $t_0 = s_1 \dots s_k = h$  and  $t_k$  defines the identity  $t_k = e$ . Rewriting  $h$  with new set of coset representatives  $t$  gives  $h = (t_0^{-1} s_1 t_1) \dots (t_{k-1}^{-1} s_k t_k)$ . We also find that  $(s_i t_i)H = s_i(t_i H) = s_i(s_{i+1} \dots s_k H) = (s_i s_{i+1} \dots s_k)H = t_{i-1} H s_i s_i t_i = t_{i-1}$ . Rewriting  $h$  with this new condition gives  $h$

$= ((s_1 t_1)^{-1} s_1 t_1) ((s_2 t_2)^{-1} s_2 t_2) \dots ((s_k t_k)^{-1} s_k t_k)$ . By definition  $t$  is the set of coset representatives, giving each  $i$  interval a factor of  $s_i^{-1} s_i$ . Any element  $h \in H$  is a product of these factors, thus the set  $\{(sa)^{-1}(sa) | a \in R, s \in S\}$  will generate  $H$ . □

The method to factorise into smaller subgroups uses a combination of Lagranges Theorem with the Orbit Stabiliser Theorem,

**Theorem 1.1** (Orbit Stabiliser Theorem). .

$$|G| = |Gx| * |G_x|$$

*applying Lagrange*

$$|Gx| = |G/G_x| = |G : G_x|$$

which simply states the size of the orbit of the group can be retrieved from the size of the group partitioned by its stabilisers. Any subgroup chain can also be completed in  $\log_2 |G|$  as the stabiliser is a subgroup for the rubiks cube group ( $G : G_x > G_x$ ) meaning  $[G : G_x] \geq 2$ , so  $|G| \geq 2|V|$  and  $|G| \geq 2^k$ . (Hulpke, 2018). So reducing the problem logarithmically can cause a major difference to understanding an algorithm to solve the cube in a certain state in the orbit, however the reduction is not that significant as  $[G : G_x]$  still remains very large. In fact for each predecesing  $G_i$  the number of generators grows exponentially,  $G_1 = 6*24$ ,  $G_2 = 6*24*22 \dots$  For an efficient solver you would need to extract which of these generators are useful to the solving problem as a large number of these are not. The algorithm has been adapted to improve on these flaws, which along with other solvers shall be mentioned later.

## Possible and Non Possible Configurations

We have the orientations of a corner cubie defined as  $Z_3$ . This is because each of corner cubie has 3 coloured faces which can be oriented differently. This makes the set of 8 corner cubies the product of all these different permutations.

$$Z_3^8 = \prod_{i=1}^8 Z_3$$

To think about the different orientations of a cubie the idea is to fix a 'starting orientation'. We know there must exist a homomorphism which takes the cubies to the correct orientation, as there exists a set of moves leading any valid configuration to the start configuration (solved). Thus using the group  $Z_3^8$ , generators of such group would be basis elements, so fixing 7 cubies give us the homomorphism below:

$$\delta : G \Rightarrow G \qquad \delta(Z_3^7) = \epsilon \qquad (16)$$

Also when considering the subgroups of  $G_{RC}$  it's necessary to define another subgroup along with the orientations of the cubies, this being  $S_8$  the permutation group of 8 elements (the 8 corner cubies). This can be defined like such, as taking any corner cubie on the cube it has 3 faces as described above which can all be alternated between each other. This being equivalent to a 3-cyclic group, denoted  $C_3$ . Which leads again to a product of 8 groups

$$C_3^8 = \prod_{i=1}^8 C_3$$

, where  $C_3^8$  is denoted as  $S_8$ . These 2 definitions above analogously follow a similar argument when considering the 12 edge cubies along the cube  $Z_2^{12}$ .

Going back to orbits and considering the difference between correct configurations, we can start by giving notation on what defines a valid configuration. At any configuration all corner cubies, as well as edge cubies, should be on orientation number corresponding to that of their group. That is,

$$\begin{aligned} e.g. x_1 = 0, x_2 = 2, \dots, x_8 = 1 \\ y_1 = 1, y_2 = 1, \dots, y_{12} = 0 \end{aligned}$$

One must also define a sign variable which states what the move has done to change where the arrangement of the corner cubies or that of the edge cubies. Define  $\tau(\in S_8)$  as the sign of the corner cubies and  $\delta(\in S_{12})$  as the sign of the edge cubies. This sign is 1 if there is an even number of transpositions, which are 2 cycle permutations, and -1 if there is an odd number.

$$\tau(x) = \begin{cases} 1, & \text{if } x \text{ contains an even number of transpositions.} \\ -1, & \text{if } x \text{ contains an odd number of transpositions.} \end{cases} \qquad (17)$$

### DEFINE K CYCLE PERM

Ignoring the center cubies as they always stay in the same position relative, a configuration is defined as  $(\tau, \delta, x, y)$ . For example an invalid configuration would be that below:



This is because there exists no set of moves to obtain the configuration shown on the right. The change of orientation of one singular cubie (from the start configuration) can only be achieved by breaking the cube, so is invalid. Given our definitions of a configuration and the labelling previous **REFERENCE LABEL ABOVE** this can be shown mathematically.

To see if one configuration can be found from another is identical to saying  $(\tau', \delta', x', y') = (\tau, \delta, x, y) * M$  e.g. applying a move  $M$  gives the different configuration. Using knowledge of orbits, define it to be the set of all possible configurations from the Rubiks Cube group  $G$ . It's known whenever a move  $M$  applied to a possible configuration is also valid then one can conclude any other valid configuration can be found from a move  $M$ . As this trivially holds for any one of the basic moves  $M = \{F, L, R, U, D, B\}$  one can conclude using basic inductive principles, that for any intermediate set of moves this will still hold as the configuration will still be in the orbit. Giving reason to saying any valid configuration of the cube can be solves with a specific set of moves. However to prove one of the fundamental theorems on the cube we still need to look at the corresponding signs of two correct configurations, hence we define the two following maps.

$$\phi_{corner} : G \rightarrow S_8 \quad \delta_{edge} : G \rightarrow S_{12} \quad (18)$$

This map all elements of the group to the subgroup  $S_8$  (Symmetric group of the corner cubies). This map is a homomorphism as it is trivially well defined, and preserves the group operation of a move e.g.  $\phi(L * L) = \phi(L) * \phi(L)$ . With this homomorphism the above objective,  $(\tau, \delta, x, y) \longrightarrow (\tau', \delta', x', y')$  from  $\tau' = \tau \phi_{corner}(M)$ , and similarly with edge pieces  $\delta' = \delta \phi_{edge}(M)$  works as from the following proof:

We know that the homomorphism is surjective, otherwise there would exist possibles moves in  $M = \{F, L, R, U, D, B\}$  taking corner cubies out of subset of corner cubie positions (contradicting our definition of the orbit of the cube group). This trivially cannot happen, a cubie with 3 faces cannot live in an edge cubie consisting of 2 faces, meaning any application of  $\phi_{corner} : G \rightarrow S_8$  will result in one of the 8 corner cubies. However to formally that this is a surjective homomorphism one must show the following:

*Proof.* It's known the symmetric group  $S_8$  is genreated by the set of 2 cycles in  $S_8$  aswell as that for any  $n$ . So to show surjectivity it's equivalent to show every 2 cycle (in  $S_8$ ) is in the image subgroup  $im_{\phi_{corner}}$ . This just means the image is entirely those 2 cycles which make up the corner cubies, and hence would mean  $sgn(\tau) = 1$ . By taking any such commutator of the cube, and using trial and inspection on a said amount of cycles a move switching position of two corner cubies (while leaving the other corners fixed) can be found. One such move is  $M = ([D, R]F)^3$  with the commutator  $[D, R]$ . This takes  $x_3$  to  $x_8$  making the cycle  $(x_3 x_8)$  while also switching edge cubies as there exists no move solely swithcing two corner cubies without affecting any of the other cubies. With this move applied to the map it gives,  $\phi_{corner}(M) = (x_3 x_8)$  thus  $(x_3 x_8)$  must lie in the image of  $\phi_{corner}$ , it just remains to show the others.

Take  $x_i, x_j$  as any two coner cubies, any corner cubie can be placed in the position of another

so there must exist a move  $p$  sending  $x_3$  to  $x_i$  and  $x_j$  to  $x_8$ . Let  $\sigma = \phi_{corner}$  and as  $\phi_{corner}$  is a homomorphism the following applies:

$$\begin{aligned}
\phi_{corner}(p^{-1}Mp) &= \phi_{corner}(p)^{-1}\phi_{corner}(M)\phi_{corner}(p) \\
&= \sigma^{-1}(x_3 \ x_8)\sigma \\
&= (\sigma(x_3) \ \sigma(x_8)) & \text{As } \sigma^{-1}(x_i \dots x_k)\sigma = (\sigma(x_i) \dots \sigma(x_k)) \\
&= (x_i \ x_j)
\end{aligned}
\quad \square$$

So for any  $x_i$  and  $x_j$  distinct in  $\{x_1, \dots, x_8\}$   $(x_i \ x_j)$  is in the image of the map, moreover  $(x_i \ x_j) \in im_{\phi_{corner}}$ .

In having a surjective homomorphism, the Group Homomorphism Theorem can be applied once again (0.1) by inspection the kernel of this group is empty thus the image is equivalently  $S_8$ . Any  $\tau \in S_8$  of this new image subgroup ( $S_8$ ) can be described as an element which moves the corner cubies from their start positions to the new positions. From the way  $\tau$  is defined it shall be either 1 or -1, using the homomorphic properties of  $S_8$  must contain an inverse element (for every element in the group), meaning applying one of the basic moves  $M$  we can get cubie  $A$  to its original position from its new position. One of these basic moves, moves 4 corner cubies, making the permutation a 4 cycle thus being an even number of transpositions  $\tau' = 1$  and thus doing  $(\tau', \delta', x', y') = (\tau, \delta, x, y) * M$  means  $\tau' = \tau\phi_{corner}(M)$ . So if  $\tau' \neq \tau$  e.g.  $\tau = -1$  applying  $M$  means  $\tau$  will now alter from an even to an odd number of transpositions thus  $\tau = -1 * -1 = 1$  and  $sgn(\tau') = sgn(\tau)$ .

There is an analogous argument with the edge cubies for  $\delta' = \delta\phi_{edge}(M)$ . Combining the analogous argument and the fact that any basic move  $M$  moves 4 corner and 4 edge cubies the following can be concluded:

*Proof.*

$$\begin{aligned}
sgn(\tau')sgn(\delta') &= sgn(\tau)sgn(\delta) \\
&= sgn(\tau)sgn(\phi_{corner}(M))sgn(\delta)sgn(\phi_{edge}(M)) & \text{Using homomorphisms above} \\
&= sgn(\tau)(-1)sgn(\delta)(-1) & \text{Both 4 cycles} \\
&= sgn(\tau)sgn(\delta)
\end{aligned}
\quad \square$$

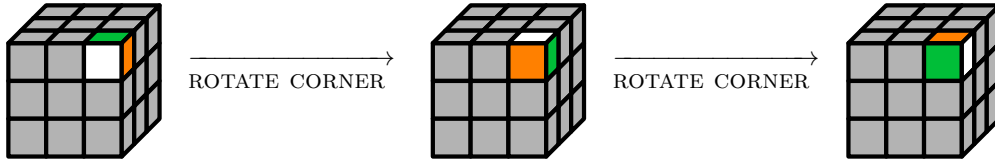
Furthermore as the start configuration is defined as (1,1,0,0) by looking at the definition of the  $sgn$ s thus any other valid configuration is also in the start configuration as shown above giving that  $sgn(\tau) = sgn(\delta)$ . This fact is fundamental in cube theory, but a full definition of what makes a correct configuration is not fully complete. For this conservation of parity between edge and corner cubies must be verified. This touches on the point made earlier in the section discussing that each cubie, edge or corner, must be associated with a number to describe the orientation of the cubie in that specific cubicle, otherwise mathematically speaking, it cannot be told if the cubes are facing in the right directions. These  $x$  and  $y$  values must obey the following rules:

$$\Sigma x_i = 0 \text{ mod } (3) \quad \Sigma y_i = 0 \text{ mod } (2) \quad (19)$$

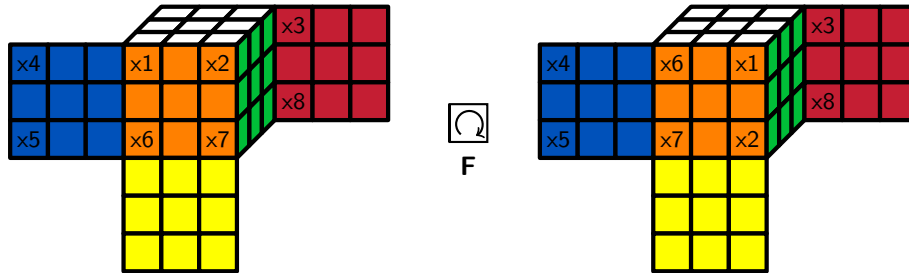
From the labelling defined previously for  $x_1$  to  $x_8$  and  $y_1$  to  $y_{12}$  the basic move  $M$  will change these values on one configuration  $((\tau', \delta', x', y') = (\tau, \delta, x, y) * M)$  in the table below (Chen, 2004):

Move	x' and y' value
D	$x_1, x_2, x_3, x_4, x_8, x_5, x_6, x_7$ $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_{10}, y_{11}, y_{12}, y_9$
R	$x_1, x_7 + 1, x_2 + 2, x_4, x_5, x_6, x_8 + 2, x_3 + 1$ $y_1, y_7, y_3, y_4, y_5, y_2, y_{10}, y_8, y_9, y_6, y_{11}, y_{12}$
U	$x_2, x_3, x_4, x_1, x_5, x_6, x_7, x_8$ $y_4, y_1, y_2, y_3, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}$
L	$x_4 + 2, x_2, x_3, x_5 + 1, x_6 + 2, x_1 + 1, x_7, x_8$ $y_1, y_2, y_3, y_5, y_1 + 2, y_6, y_7, y_4, y_9, y_{10}, y_{11}, y_8$
F	$x_6 + 1, x_1 + 2, x_3, x_4, x_5, x_7 + 2, x_2 + 1, x_8$ $y_1, y_2, y_8 + 1, y_4, y_5, y_6, y_3 + 1, y_{11} + 1, y_9, y_{10}, y_7 + 1, y_{12}$
B	$x_1, x_2, x_8 + 1, x_3 + 2, x_4 + 1, x_6, x_7, x_5 + 2$ $y_6 + 1, y_2, y_3, y_4, y_1 + 1, y_9 + 1, y_7, y_8, y_5 + 1, y_{10}, y_{11}, y_{12}$

The method in which the corresponding x's and y's have been added by a number between mod 2 or mod 3 is defined below. Assume the below cube consists of a valid configuration, where there exists a move sequence which rotates the top front face corner cubie in its cubicle only.

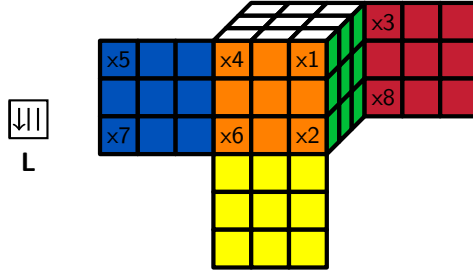


Also assume the cubie fits in the cubicle correctly in the first cube, e.g. its in the correct position and orientation currently. Each time a move is applied and the cubie is rotated from its correct orientation there will be an addition of 1 to preserve notational parity. For example let the cubie =  $x_2$ , when rotate corner sequence is applied the orange moves to the white facet clockwise 1 face, so the new  $x'_2$  becomes  $x_2 + 1$ . If the sequence was applied twice to go from the first to the third the new  $x'_2$  becomes  $x_2 + 2$  as there are 2 clockwise movements. This is also similar for the edge pieces, but for only 2 changing faces there will only ever be a +1 or +0 (cycles back). As an example the front face turn is shown below.



Where in the solved position x1 has a white face up, blue face leftwards and orange face frontwards. After the permutation (1,2)(2,7)(7,6),(6,1), it now lives in the x2 cubicle where the blue





face is now upwards, the blue face is 2 clockwise positions from initial (white face), thus  $x_1 + 2$ . Same applies with other cubies affected giving after a F move  $x_1 + 2, x_2 + 1, x_6 + 1, x_7 + 2$ , complying with the table above. Applying an additional L move takes (5,4)(4,6)(6,7),(7,5) to their new positions. Giving  $x_4 + 2, x_5 + 1, x_6 + 2, x_7 + 1$  and the remaining corner cubies unchanged. Note these x's are taken as permutes from the start configuration not for the previous move.

So checking parity of all the corner cubies in this for the new configuration  $(\tau', \delta', x', y')$  under the move FL:

$$x' = x_1 + 2, x_2 + 1, x_3 + 0, x_4 + 2, x_5 + 1, x_6 + 2, x_7 + 1, x_8 + 0 \quad (20)$$

$$\Sigma x'_i = \Sigma x_i + 9 = \Sigma x_i \pmod{3} \quad (21)$$

This will hold for any of the moves as shown in the parity table, and therefore any subsequent set of moves. In fact given the above information the conservation for the parity of corner and edge cubies can already be shown.

**Theorem 1.2** (Parity of Edge and Corner Cubies). *If  $(\tau, \delta, x, y)$  is a valid configuration then  $\Sigma x_i = 0 \pmod{3}$   $\Sigma y_i = 0 \pmod{2}$*

Because its shown any perumation of moves leaves the new configuration in the same orbit of the start configuration (1,1,0,0) and as  $\Sigma x'_i = \Sigma x_i \pmod{3}$  the theorem must hold.

Now the previous conditions have given the ability to characterise any valid configuration of a rubiks cube state. Let us define these conditions into the following theorem.

**Theorem 1.3** (Fundamental Theorem of Cube Theory). *Let  $\tau \in \mathbb{Z}_3^8$ ,  $\delta \in \mathbb{Z}_2^{12}$ ,  $x \in S_8$ ,  $y \in S_{12}$  make up a valid configuration  $(\tau, \delta, x, y)$  if and only if:*

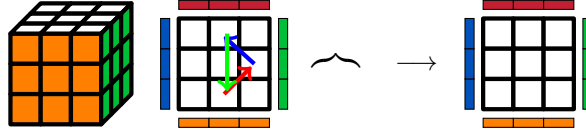
1.  $\text{sgn}(\tau) = \text{sgn}(\delta)$  (Parity of Permutaions)
2.  $\Sigma x_i = 0 \pmod{3}$  (Orientation of Corners)
3.  $\Sigma y_i = 0 \pmod{2}$  (Orientation of Edges)

*Proof.* In fact this foward direction has already been shown above in constructing what the definition of what makes a configuration above in the section. So the converse is left to show in this proof:

Assume there exits a configuration  $C = (\tau, \delta, x, y)$  which satisfies 1.,2.,3.

1. implies that the signs are equal meaning equal parity of permutations, meaning that they're either -1 (odd number of permutations) or 1 (even number of permutaions). In fact this proof just highlights what the surjectiveness of the homomorphism in 18, as this says any corner cubie can be

placed in the place of another one until the correct position is found). By following from the proof this means  $\tau = 1$  in the configuration so to show parity, it must be now shown  $\delta = 1$  for equality. Recalling the section on alternating and symmetric groups,<sup>3</sup> the kernel is entirely  $A_n$ , which is generated by the set of 3-cycles in  $S_n$  in other words the odd transpositions (as the 1 cycle is trivial it is not considered in the explanation). Then for a map such as  $\phi_{edge}|_{ker(\phi_{corner})} : ker(\phi_{corner}) \rightarrow S_{12}$  the image of it should just be the set of 3 cycles from the result of  $\phi_{edge}(ker(\phi_{corner}))$  on an element from  $ker(\phi_{corner})$  which is just the elements of the alternating group  $A_8$ . Note the function is restricted to  $ker(\phi_{corner})$  to show if  $\tau = 1$  the same applies with  $\delta$ . So to show the parity is preserved is equivalent to showing the image (every 3 cycle) of this map is contained within  $A_{12}$ . Take a cycle permuting 3 edge pieces, say  $(y_1, y_2, y_3)$  with the move  $M = R^2 U F B^{-1} R^2 F^{-1} B U R^2$



Where the red arrow is from  $x_1$ , blue from  $y_2$  and green from  $y_3$  complying with the usual labelling. With this cycle  $(y_1, y_2)(y_2, y_3)$  there is an even number of even number of 2 cycle permutations (transpositions), thus will have  $sgn(\delta) = 1$ . Any of the remaining edge cubies for  $y_i$  (4 to 12) will be able to substitute for  $a_3$  creating their respective cycles  $(y_1, y_2, y_4)$ ,  $(y_1, y_2, y_5) \dots$ ,  $(y_1, y_2, y_{12})$ . This is because there exists any move which will take  $y_i$  to  $y_3$  without affecting the other two edge cubies. Call this move  $p$ , and substitute  $M$  for  $pMp^{-1}$  and we have the desired result. Note that this  $p$  will always be less than or equal to two of the basic moves just from the construction of the cube. This now gives  $M \in (ker(\phi_{corner}))$  so  $\phi_{edge}(M) = (y_1 y_2 y_3)$ . Labelling the new move as  $M' = pMp^{-1}$ ,  $M'$  can be split into disjoint cycle decomposition  $(y_i y_j y_k)$ , as well giving  $M' \in ker(\phi_{corner})$  so  $\phi_{edge}(M') = (y_i y_j y_k)$  for any given  $i, j, k \in \{1, \dots, 12\}$  where  $i, j, k$  are distinct. So as for any edge cubie  $i, j, k$ ,  $(y_i y_j y_k)$  is in the image of the map, i.e.  $\in im_{\phi_{edge}|_{ker(\phi_{corner})}}$  thus we have reached condition above. So in correspondance with the previous proof of surjectiveness, again  $sgn(\delta) = 1$ . So now for configuration  $C$ , it must be such that  $(1, \delta, x, y)$   $\delta = 1$ , hence  $\tau = \delta = 1$  giving us parity between permutations which concludes the proof of 1. For 2. and 3. it's just left to show that the orientation of the corners and edges always sums to 0 (mod 3) and 0 (mod 2) respectively. As in equation 11 a move was found to orient corner cubies  $x_1$  and  $x_2$  without affecting any of the other corner cubies. This can be applied to any two such corner cubies  $(x_i x_j)$  rotating  $x_i$  clockwise one face and  $x_j$  anti-clockwise one face. So to first show 2. do an assumption by contradiction.

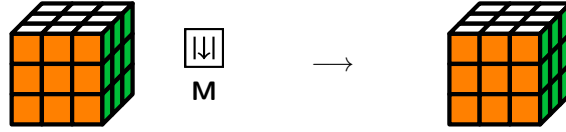
*Proof.* Suppose the Rubiks Cube is in a configuration where at least two corner cubies have the wrong orientation. By the above we can implement a move rotating  $x_i$  clockwise and  $x_j$  counter-clockwise. Therefore we the application of this move  $x$  amount of times one can ensure  $x_i$  has the correct orientation. So now there is one fewer cubie with an incorrect orientation, as doing those moves would not have affected any of the other corner cubies. Repeating this action across the rest of the unoriented cubies leaves in a state with at most one corner cubie which is incorrectly oriented. But as it's already been shown in equation 21 and the following explanation as well as theorem 1.2 that  $\Sigma_{x_i}' = \Sigma_{x_i} = 0 \pmod{3}$  for a move on a valid configuration. Thus as there are 7  $x_i'$  with correct orientation as  $\Sigma_{x_i}' = \Sigma_{x_i} = 0$  the only possible value for the last  $x_i'$  must also be 0,

therefore proving 2. □

Now to show 3. implement a similar argument as such:

*Proof.* Like for the corners there exists a move which orients two corner cubies. This move is  $M = LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}B^{-1}LR^{-1}U^{-1}$

For notation purposes include the slice move  $M_R$  for an easier description of the move  $(M_R U)^4 (M_R U^{-1})^4$ . This slice move rotates the middle slice clockwise as such: So this move M like above has disjoint



cycle decomposition  $(y_2 y_2^{-1})(y_4 y_4^{-1})$ . So for any two distinct edge cubies  $y_i, y_j$  there exists a move sending  $y_2^{-1}$  to  $y_i$  and a move sending  $y_4^{-1}$  to  $y_j$ . Let this move be denoted as  $p$ , and thus similar to the above argument  $pMp^{-1}$  changes the orientation of the two edge cubies  $y_i, y_j$  without affecting any other edge piece. Another proof by contradiction supposing the cube is in a state where at least two edge pieces have an incorrect orientation identical to the argument for corner pieces leads to the conclusion of 3. □

As all 3 arguments to the theorem have been proved there is now a conclusive proof on what makes and what is a valid configuration of the rubiks cube. □

## Applications

Mathematically to talk about these groups further and to understand the illegal rubiks cube group it's sensible to introduce normal subgroups, semi-direct products and wreath products.

### Normal Subgroup

A subgroup  $H$  of  $G$  is normal if  $gH = Hg$ ,  $\forall g \in G$  this is denoted as  $H \trianglelefteq G$  and  $H \triangleleft G$  if  $G \neq H$

### Semi-Direct Product

Given group  $G$ , subgroup  $H$ , normal subgroup  $N \triangleleft G$  and that the following hold,

- $G$  is the product of subgroups  $N, H$  such that  $G = NH$  where  $N \cap H = e$  the identity of  $G$
- $\exists$  a homomorphism  $G \rightarrow H$  that is the identity on  $H$  whose kernel is  $N$ .

Then  $G = N \rtimes H$  is a semi-direct product

### Wreath Products

The Wreath products of two groups  $G$  and  $H$  below:

- $G^H$  is the set of all functions defined on  $H$  with values in  $G$ , where  $G^H$  is an automorphism
- Let  $X$  be a finite set, where  $G^X$  is acted upon by  $H$ , this is just functions taking non identity values on a finite set of points  $X = \{x_1, x_2, \dots, x_p\}$ . So is trivially smaller than the set of all functions.

$$G^X \wr H = G^X \rtimes H \quad (22)$$

is then the wreath product of  $G$  by  $H$ . So is just the semi direct product of  $p$  copies of  $G$  by  $H$  (of Mathematics, 2014). To further show these two properties the following examples firstly on the additive group  $(\mathbb{Z}, +)$ .

Let  $G = \mathbb{Z}_5 = \{0, 1, 2, 3, 4, 5\}$  and  $H = \{1, 2, 3\}$ , and so  $\forall g \in G, g + H = H + g$  as addition in the group of integers is commutative,  $H$  is thus a normal subgroup of  $G$ .

Secondly considering the group of symmetric transpositions  $S_n$ , in semi-direct product notation it can be written as  $S_n = A_n \rtimes \langle (12) \rangle$ . This can be shown simply by following the conditions in the definition. Disjoint subgroups  $A_n \cap \langle (12) \rangle = e$ . For  $a \in S_n$  and  $b \in A_n$ , as  $b$  are the even cycle permutations  $\text{sgn}(b) = 1$  thus  $aba^{-1} \in A_n$  as with homomorphic properties there is  $\text{sgn}(aba^{-1}) = \text{sgn}(a)\text{sgn}(b)\text{sgn}(a^{-1}) = s^2 = 1$ . Therefore  $A_n \triangleleft S_n$  hence  $S_n = A_n \rtimes \langle (12) \rangle$  as above. Finally take the two groups  $G = \mathbb{Z}_2$ ,  $H = S_3$  and the set  $X = \{1, 2, 3\}$ . The wreath product of  $G$  by  $H$  is  $\mathbb{Z}_2^3 \wr S_3$  with elements  $\{(0, 0, 0)\sigma, (1, 0, 0)\sigma, (0, 1, 0)\sigma, (0, 0, 1)\sigma, (1, 1, 0)\sigma, (1, 0, 1)\sigma, (1, 1, 1)\sigma\}$  where  $\sigma \in S_3$ .

### Illegal Rubiks Cube Group

This can be implemented into the groups already discussed in the project. As mentioned in the context of the cube, the group of corners and edges can be described as to being in separate orbits of the cube group orbit. Where the group of corner cubies, let's say  $C_{\text{corner}}$  can be constructed from

the identities already defined.  $C_{corner}$  will act on the set of corner cubies  $S_8$  to obtain the corner positions and to obtain the corner orientations  $\mathbb{Z}_3^8$  it just performs the direct product between the two. As by following the definition the group of orientations is a normal subgroup for the corners it follows that the group of corner cubies is  $C_{corners} = (S_8 \wr \mathbb{Z}_3^8)$ . A similar argument can be made to find that the group of edges is  $C_{edges} = (S_{12} \wr \mathbb{Z}_2^{12})$ .

The rubiks cube group is made up of these separate orbits (the centre cubies can be disregarded as they do not change position) so the rubiks cube group is made out of their direct product  $G_{RC} = C_{edges} \times C_{corners}$  thus  $G_{RC} = (S_{12} \wr \mathbb{Z}_2^{12}) \times (S_8 \wr \mathbb{Z}_3^8)$ .

Earlier the rubiks cube group was said to have  $4.3 * 10^{19}$ , these are actually just the valid configurations used computationally when algorithms such as using pre-made solver algorithms. So what was defined as  $G_{RC}$  is actually the illegal rubiks cube group  $I = G_{RC}$  as the total number of configurations here are:

$$I = |\mathbb{Z}_2^{12}| |\mathbb{Z}_3^8| |S_{12}| |S_8| = 12! * 8! * 3^7 * 2^{11} \quad (23)$$

Which is around  $86 * 10^{19}$  configurations, what makes a portion of these configurations illegal is the double counting that takes places. This is because only one third of the permutations have the correct corner cubie configuration. Also half of these permutations have the correct edge cubie configurations and half of these such configurations have the correct parity's for their signs. This sum is basically achieved for all cases where the fundamental theorem is not met, thus the amount of valid configurations is actually near a 12th of the total number,  $4.3 * 10^{19}$  configurations.

### Legal Rubiks Cube Group

The official legal rubiks cube group  $G_{RC}$  is made up of the cube orientations and the cube permutations, where the intersection of these two is the identity, it follows by definition the rubiks cube group is the semi-direct product of the two.

$$G_{RC} = C_{orientations} \rtimes C_{permutations} \quad (24)$$

Where  $C_{orientations}$  is just  $\mathbb{Z}_2^{12} \times \mathbb{Z}_3^8$  as rotations groups under integers are abelian and such following rotations determine the orientation of previous rotations. The  $C_{permutations}$  is more complex, so firstly think of this permutation group on the cube as a product of two subgroups. The first being the group of permutations on the 8 corner cubies and the second being on the 12 edge cubies. Due to 1.3(1) there parity must be equal. So as the alternating group contains the even permutations the direct product  $A_8 \times A_{12}$  contains half the permutations in the permutation group. As any combination of even permutations is even it follows from the definition that this identity is a normal subgroup of the permutation group. For the second half of this group consider the group  $\{e, (ur, uf)(urf, urb)\}$ . Now the permutation group can be expressed as a semidirect product between these two groups. The identity element  $e$  is chosen if both permutations are already even and  $(ur, uf)(urf, urb)$  is chosen if both permutations are odd (Beeler, 2016). Trivially the group  $\{e, (ur, uf)(urf, urb)\}$  is isomorphic to  $\mathbb{Z}_2$  with two elements one being the identity  $e$ . Combining all these facts to the legal rubiks cube group gives us:

$$G_{RC} = C_{orientations} \rtimes C_{permutations} = (\mathbb{Z}_2^{12} \times \mathbb{Z}_3^8) \rtimes ((A_8 \times A_{12}) \rtimes \mathbb{Z}_2) \quad (25)$$

## Possible Extension- CRAN cubing package

For the section relating gods number and efficiency to actually solving the cube, it will be implementing the CRAN cubing package (seesource). From this it will aid in the explanation about ways to solve the cube as well as showing how the mathematics behind the cube ties in with the programming. After installing the CRAN package and using the R command to further access specific packages within CRAN , the cube functions can finally be accessed. The notation of defining the cube in terms of an array is as such:

```
ellisp97@ellisp97: ~/Desktop/rubikscube/cubing
File Edit View Search Terminal Help
> hello.cube
$cp
URF UFL ULB UBR DFR DLF DBL DRB
 1  2  3  4  5  6  7  8

$ep
FR FL BL BR UR UF UL UB DR DF DL DB
 1  2  3  4  5  6  7  8  9 10 11 12

$co
URF UFL ULB UBR DFR DLF DBL DRB
 0  0  0  0  0  0  0  0

$eo
FR FL BL BR UR UF UL UB DR DF DL DB
 0  0  0  0  0  0  0  0  0  0  0  0

$spor
U R F D L B
1 2 3 4 5 6
```

Entering the command `hello.cube` displays how the cube is stored with a similar notation to how it's labelled earlier in the project. Where **cp,ep,co,eo** stand for corner/edge permutation and orientation (where the cubicles live in the cubie).

INSERT SOME SORT OF CAMPRISON TO DO WITH LABELLING

Visual aid however is important as without this it becomes hard to see what's actually happening to the cube. This comes in 2d and 3d plots, with the commands `plot(yourCube)` and

`plot3d(yourCube)` once defined (To enable the use of a 3D plot with RGL, start the RGL device in the R command).

Using a construction like so allows the user to input any configuration of a cube into the system, whether it's valid or invalid (in terms of solvability defined previously) so long as it obeys methods of input e.g.

```
1 >yourCube = cubieCube("UUUUUUU RLLRLLR BBFFFFB DDDDDDD LRRLLRL FFBBBBF")
2 >plot(yourCube, numbers = TRUE)
```

and then can plot in usual way (including numbers = TRUE displays the cubie positions on the cube like so). A function which is imperative for the input of these cubes is **is.solvable**. When on input of a cube previously defined will return a boolean value depending on whether the configuration entered is correct or not.

[INSERT LINK ON AMOUNT OF FALSE CUBIES WITH TRUE CUBIES USING FUNC\(sum\(sapply\(randCube\(100, solvable = FALSE\), is.solvable\)\)\) , USING COMBINATORIAL ARGUMENT](#)

Furthermore when a cube which has an invalid configuration has been input,

```
1 >is.solvable(yourCube, split = TRUE)
2
3   parity   co   eo
4   TRUE   TRUE FALSE
```

is solvable will tell you the condition of how yourCube fails to be solvable.

[INSERT LINK TO HOW THIS RELATES TO MOD 3 STUFF](#)

Using the following command a user can create their own move by separating the standard moves with spaces (or even separate lines). This has uses and can be used in conjunction with the is.solvable to see if a certain set of moves can take one configuration to the start configuration (solved).

```
1 > yourCube <- getMovesCube(scan(what = character()))
2
3 1: D2 F2 U F2 D R2 D B L' B R U L R U L2 F L' U
4 20:
5 19 moves read
6
7 > mv <- scan(what = character())
8 1: D2 F2 U F2 D R2 D B L' B R U L R U L2 F L' U
9 20:
10 19 moves read
11
12 > result <- move(yourCube, mv)
13 > is.solved(result)
14
15 [1] TRUE
```

[INSERT STUFF RELATING ON ANIMATION E.G. WR MOVE ANIMATE\(ACUBE,MV\)](#)



A question must be asked on the efficiency of this 'solver', how it works and how fast it can be done. The solver used in the `is.solveable` function is called the *Kociemba Solver*. This algorithm was created by Herbert Kociemba in 1992 which is an adapted version of the Thistlethwaite algorithm often referred to as the breakthrough for cube solvers(Thistlethwaite, 1981) . So to understand how efficiency works between solvers this algorithm must be considered first.

## Thistlethwaite's Algorithm

The idea of this was to create a *Divide and Conquer* style implementation, which essentially means to divide one big problem (solving the cube) into many different smaller subproblems. It uses the main concepts of group theory explained above, while utilising complex computer searches on very large lookup tables. The cube group  $\mathcal{G}_{RC}$  is split up into the following sequence of subgroups.

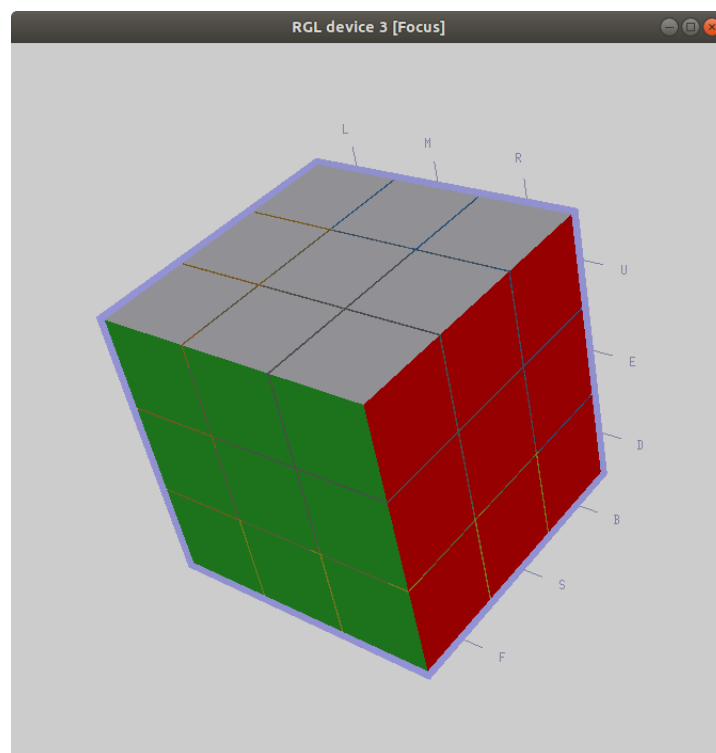
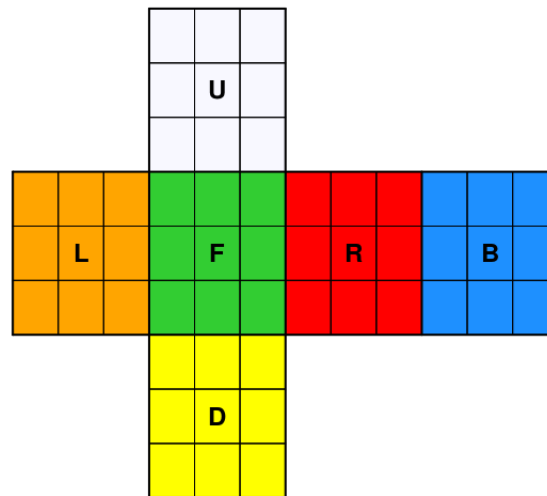
$$\mathcal{G}_{RC} = \begin{cases} G_0 = \langle L, R, F, B, U, D \rangle. \\ G_1 = \langle L, R, F, B, U^2, D^2 \rangle. \\ G_2 = \langle L, R, F^2, B^2, U^2, D^2 \rangle. \\ G_3 = \langle L^2, R^2, F^2, B^2, U^2, D^2 \rangle. \\ G_4 = 1. \end{cases} \quad (26)$$

This technique allows the cube to be solved in a maximum of 52 moves. Using the smaller subgroups he restricts the possible space of moves which can be made, this works by moving down the chain of  $G_0$  to  $G_4$

## References

- Beeler, R. A. (2016). Group theory and the rubiks cube. Retrieved from <http://faculty.etsu.edu/gardnerr/4127/algebra-club/rubik-talk2a.pdf>
- Chen, J. (2004). Group theory and the rubik's cube.
- Hulpke, A. (2018). Computational group theory. Retrieved from <http://www.math.colostate.edu/~hulpke/talks/CR/CR1.pdf>
- Jaap. (1981). Computational group theory. Retrieved from <https://www.jaapsch.net/puzzles/schreier.htm>
- Limited, R. C. B. (2017). The history of the rubiks cube. Retrieved from <https://uk.rubiks.com/about/the-history-of-the-rubiks-cube>
- of Mathematics, E. (2014). Wreath products. Retrieved from [http://www.encyclopediaofmath.org/index.php?title=Wreath\\_product&oldid=35297](http://www.encyclopediaofmath.org/index.php?title=Wreath_product&oldid=35297)
- record holders. (2017). Rubiks cube world records. Retrieved from <http://www.recordholders.org/en/list/rubik.html>
- Singmaster, D. (1981). Notes on rubiks magic cube.
- Thistlethwaite, M. (1981). The thistlethwaite algorithm. Retrieved from <https://www.jaapsch.net/puzzles/thistle.htm>
- Wolfram. (2018). Permutation groups. Retrieved from <http://reference.wolfram.com/language/tutorial/PermutationGroups.html>

R Graphics: Device 2 (ACTIVE)



			U1	U2	U3							
			U4	U5	U6							
			U7	U8	U9							
L1	L2	L3	F1	F2	F3	R1	R2	R3	B1	B2	B3	
L4	L5	L6	F4	F5	F6	R4	R5	R6	B4	B5	B6	
L7	L8	L9	F7	F8	F9	R7	R8	R9	B7	B8	B9	
			D1	D2	D3							
			D4	D5	D6							
			D7	D8	D9							