Mathematics of the Rubik's Cube:

Finding God's Number of the Pocket Cube

Author: Kheeran K. Naidu

Level H/6 20CP

Supervisor: Professor Francesco Mezzadri

13^{th} May 2019

This project complies with the guidelines set out in the Project Handbook 2018-19.

Acknowledgement of Sources

For all ideas taken from other sources (books, articles, internet), the source of the ideas is mentioned in the main text and fully referenced at the end of the report.

All material which is quoted essentially word-for-word from other sources is given in quotation marks and referenced.

Pictures and diagrams copied from the internet or other sources are labelled with a reference to the web page or book, article etc.

Signed 

Date 13/05/2019

Contents

Abstract

In this paper, we will be studying some different approaches to representing the structure of a group. In particular, we compare generators with generator relations to direct and semi-direct products. We apply these methods to the Pocket (2x2x2) and Rubik's (3x3x3) cubes and see the benefits of each of the methods. We will discuss the question of the more reasonable sized Pocket Cube, which was invented, originally by Larry Nichols and patented in 1972 [23], but popularised by Ideal Toy Company [21]. We find, using the generators of the group to build the Cayley Graph of the Pocket Cube Group, that God's number is 11 using the half-turn metric.

1 Introduction

Games and puzzles have always been a key learning tool for children of all ages. The intricacies involved in solving some of these puzzles is said to provide children with a collection of analytical skills [6]. Many of these puzzles provide a challenge to children, however, some, the Rubik's Cube in particular, also provide a challenge for well regarded mathematicians.

The Rubik's Cube is a 3D puzzle invented by Ernő Rubik in 1974. Since its inception the puzzle has become a worldwide phenomenon. Many mathematicians and computer scientists have attempted to unravel the secrets of the cube, however, one question has taken over 3 decades to answer; *what is God's Number*? What is the minimum number of moves required to solve any valid configuration of the Rubik's cube? It is so called 'God's Number' because it used to be thought that this number was known only to God.

The manner of counting moves that we will use is that of the half-turn metric [20]. It is the manner of counting most commonly used in western documentation of the Rubik's Cube. In group theoretic language, the problem of finding God's Number is analagous to that of finding the maximum edge distance between vertices of the Cayley Graph of the Rubik's Cube group; it was found to be 20 using the half-turn metric.

The first attempts at finding God's number were by taking the worst case scenario of solving algorithms of the cube, and using them to set the upper bound. The first notable one was by David Singmaster in 1979 [1] which was around 80 or so [14]. He also proved by a simple counting argument that some positions required at least 18 moves to solve, thus setting the lower bound of 18 on God's Number.

The first person to make a significant breakthrough was Morwen Thistlethwaite in 1981. He devised a method which significantly decreased God's Number to an upper bound of 52 moves by using a chain of subgroups and their cosets [2]. For the next decade, there wasn't much activity in the lowering of the upper bound of God's Number for the Rubik's cube.

The next big lowering of the bound was by Michael Reid in 1995 by analysing Kociemba's two-phase algorithm [3] introduced in 1992 by Herbert Kociemba, which was a fascinating new cube solving algorithm that found near-optimal solutions rapidly; he lowered the upper bound to 29 moves [14]. Michael Reid, also in 1995, increased the lower bound to 20 by proving the existence of the "superflip" position [4]. Again, the next decade was silent, with very little work being done to find God's Number. In 2005, the birth of Rubik Cubism [24][8] re-kindled research into God's Number. For the next 5 years the upper bound was continually lowered and in 2010 it was proved to be 20 [14].

Finally in 2013, the paper was published by Tomas Rokicki, Herbert Kociemba, Morley Davidson and John Dethrudge proving that God's Number is in fact 20 for the Rubik's cube (3x3x3) by counting moves using the half-turn metric. Ultimately this proof required 35 years of CPU time [15]. This number is yet to be found for cubes such as the Rubik's Revenge (4x4x4) or larger, so it's nomenclature still has some relevance.

The motivation for this paper is to show that understanding a problem using mathematical structures, in this case group structures, allows us to find and prove interesting facts which can then be used to gain insight on and/or solve the problem. We will see that some ways of presenting the structure are more informative than others by representing the group structure with generators and generator relations, and also using direct-products and semi-direct products. In this case we will be understanding the underlying mathematical group structure of the Pocket Cube (2x2x2 miniature Rubik's Cube), and using that to

find God's Number; using the half-turn metric we find that to be 11. We will also look at the structure of the Rubik's Cube (3x3x3) and the similarities it has with the Pocket Cube.

We will define the general rules and goals of the cubes, and describe the differences between the variations which we will be studying; the Pocket Cube and Rubik's Cube. We will approach the construction of the Pocket Group and Rubik's Group using generators and generator relations, and using the direct products and semi-direct products of subgroups of the groups respectively. Subsequently, we will look at the question of God's Number and the ways that have been used to estimate and find it.

2 Preliminaries

Throughout this paper we will mainly be using the Definitions, Propositions and Theorems introduced in this section. If you feel you have a good understanding of these concepts feel free to skip this section as it is meant for readers who may not have a good grasp of them.

We will be following the convention of reading from left to right, unless otherwise specified; this means that we will be using the *right* function composition and *right* group action, instead of the otherwise used *left* function composition and *left* group action.

2.1 Groups

Definition 2.1.1. [5] A group is a set G together with a binary operation $\circ$, often represented as a tuple $(G, \circ)$, such that the following axioms hold:

$\forall x, y, z \in G$,

- there is *closure* in G under the binary operation, $x \circ y \in G$;
- the *associative* property holds on $(G, \circ)$, $(x \circ y) \circ z = x \circ (y \circ z)$;
- there exists an *identity* element $e \in G$, such that $e \circ x = x \circ e = x$;
- there exists an *inverse* for each element such that $x \circ x^{-1} = e = x^{-1} \circ x$.

Definition 2.1.2. [19] The cardinality of a group $(G, \circ)$, called its **order** and denoted by $|G|$, is the number of elements in the group. G is said to be **finite** if $|G| \in \mathbb{N}$ and **infinite** otherwise.

Definition 2.1.3. [19] Let a be an element of group G. If $a^n = e$ for some $n \in \mathbb{N}$ then the smallest such n is called the **order** of a, denoted by $|a|$. If no such n exists then we say that a has **infinite order**. We note that $|a| = 1$ iff $a = e$.

Definition 2.1.4. [12] A group (G, $\circ$) is abelian iff $\forall x, y \in G, x \circ y = y \circ x$. In other words, the binary operation is commutative. The examples 2.1.5 and 2.1.6 are also abelian groups.

Example 2.1.5. A simple example of an infinite group is the integers under addition, $(\mathbb{Z}, +)$. It is easy to show that it satisfies each axiom in Definition 2.1.1 [13].

Example 2.1.6. A finite group is the integers under multiplication modulo p, $(\mathbb{Z}/p\mathbb{Z}, \times)$ denoted by $\mathbb{Z}_p^\times$ where p is prime. $|\mathbb{Z}_p^\times| = |\{1, ..., p-1\}^\times| = \Phi(p) = p - 1$ by the *Euler function* [12]. We also have that $e = 1 \in \mathbb{Z}_p^\times$ and $\forall x \in \mathbb{Z}_p^\times, x \neq 1, |x| = p - 1$ by *Euler's Theorem* [12] therefore $x^{-1} = x^{p-2}$.

Example 2.1.7. $(\mathbb{R}, \times)$ is not a group because $0 \in \mathbb{R}$ does not have an inverse.

Example 2.1.8. An example of a non-abelian group is the set of 2x2 matrices under matrix multiplication, $(\mathbb{R}^{2x2}, \times)$ since $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 2 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 3 & 2 \end{pmatrix}$.

2.2 Subgroups & Generators

Definition 2.2.1. [5] A subgroup $(H, \circ)$ of a group $(G, \circ)$ is a subset $H \subseteq G$, which satisfy the axioms of a group (Definition 2.1.1) under the same binary operation as group G. We write $H \leq G$ to indicate that H is a subgroup of G.

Definition 2.2.2. [19] Let G be a group and $S \subseteq G$. Let $X = \{H | H \leq G and S \subseteq H\}$ be the collection of subgroups of G containing S. Then the subgroup

$$< S >:= \bigcap_{\forall H \in X} H \tag{1}$$

of G is called the *subgroup of G generated by S* and is the smallest subgroup of G containing S.

Definition 2.2.3. [19] Let G be a group. A subset $S \subseteq G$ is a **generating set** of G if $G =< S >$, and the elements of S are called generators of G. We say that G is **finitely generated** if there exists a finite subset $S \subseteq G$ such that $G =< S >$; if $S = \{a_1, a_2, ..., a_n\}$ we write $G =< a_1, a_2, ..., a_n >$.

Definition 2.2.4. [19] A group G is **cyclic** if there is an element $g \in G$ such that $G =< g >$. Such an element g is called a **generator** of G.

Example 2.2.5. Let $G = \mathbb{Z}_8^+$ and $H = \{0, 4\}^+$. $0, 4 \in \mathbb{Z}_8 \implies H \subseteq G$. $0 + 0 = 4 + 4 = 0, 0 + 4 = 4 + 0 = 4 \in H \implies H$ is *closed* under addition, is *associative* and that each element is its own *inverse* with 0 as the *identity*. Therefore $H \leq G$. We note that $H \cong \mathbb{Z}_2^+$ (refer to Definition 2.7.3).

Example 2.2.6. Let $G = \mathbb{Z}_8^+$. By *Lagrange's Theorem* [12] the order of the subgroups H_i of G must divide the order of G therefore the order of the subgroups H_i are the factors of $|G|$; which are $1, 2, 4, 8$. We then have that the subgroups of G are

$$H_1 = \{0\}^+, \tag{2}$$
$$H_2 = \{0, 4\}^+, \tag{3}$$
$$H_3 = \{0, 2, 4, 6\}^+, \tag{4}$$
$$H_4 = \{0, 1, 2, 3, 4, 5, 6, 7\}^+ = G. \tag{5}$$

Then, by Definition 2.2.2 the elements $x \in G$ generate the following subgroups;

$$< 0 > = H_1, \tag{6}$$
$$< 1 > =< 3 >=< 5 >=< 7 >= G, \tag{7}$$
$$< 2 > =< 6 >= H_3, \tag{8}$$
$$< 4 > = H_2. \tag{9}$$

We say that the elements $1, 3, 5, 7$ each generate the entire group G.

2.2.1 Generator Relations

We normally present groups and their generators without explicitly specifying the generator relations of the group. However, when defining a group, we can define it using its set S of generators, as seen in Example 2.2.6, along with its set R of **generator relations**, or sometimes defining relations [12]. This gives us a better understanding of the group structure.

Definition 2.2.7. Let $G =< S >$ be a group. A *generator relation* of the group is an element of the group such that the sequence of generator moves which make up the word of the group element can be replaced by the identity of the group.

Example 2.2.8. Let D_{2n} be the dihedral group of order 2n. We can represent this group with the generating set $S = \{a, b\}$ and the relation set $R = \{a^n, b^2, (ab)^2\}$ such that

$$D_{2n} =< a, b : a^n = b^2 = (ab)^2 = e > . \tag{10}$$

The dihedral group is the group of symmetries of a regular n-sided polygon where the element $a \in D_{2n}$ is an anticlockwise rotation by $\frac{360}{n}^\circ$ and the element $b \in D_{2n}$ represents a reflection in the line through vertex 1 and the center of the polygon [16]. So it makes sense that a^n a rotation through 360° and b^2 a reflection through the same axis twice are the identity.

Example 2.2.9. Let group $G = (\mathbb{Z}_2[x], +) = \{a_0 + a_1x + ... + a_nx^n : a_i \in \mathbb{Z}_2, n \in \mathbb{N}\}^+$. We can represent this group with the infinite generating set $S = \{1, x, x^2, ...\}$ and the infinite relation set $R = \{2x^n : \forall n \in \mathbb{N} \cup \{0\}\}$ such that

$$G =< 1, x, x^2, ... : \forall n \in \mathbb{N} \cup \{0\}, 2x^n = 0\} > . \tag{11}$$

2.3 Cosets

The cosets of groups are useful for their property that they partition groups in to equally sized sets

Definition 2.3.1. For $H \leq G$ and $g \in G$, the set $Hg = \{hg : h \in H\}$ is called the *right coset* of H in G denoted by $H\backslash G$.

Example 2.3.2. Take the dihedral group $G = D_8$ of a 4-sided regular polygon. Let $H =< a >$ be a subgroup of D_8. The right cosets of $H\backslash G$ are

$$H = \{he : h \in H\} = \{e, a, a^2, a^3\} \tag{12}$$

$$Hb = \{hb : h \in H\} = \{b, a, a^2b, a^3b\} \tag{13}$$

2.4 Group Actions & Orbits

Definition 2.4.1. [12] Let G be a group and X be a non empty set. We say G acts on X by the *right group action* if there exists a map $X \times G \to X, (x, g) \mapsto x \cdot g$ such that, $\forall x \in X$ and $\forall g, h \in G$,

1. $x \cdot (gh) = (x \cdot g) \cdot h)$, and
2. $x \cdot e = x$, where $e \in G$ is the identity element of group G.

Definition 2.4.2. [5] A binary relation $\sim$ on X is an **equivalence relation** on X if $\sim$ satisfies the following properties: $\forall x, y, z \in X$

- (reflexivity) $x \sim x$;
- (symmetry) if $x \sim y$ then $y \sim x$; and
- (transitivity) if $x \sim y$ and $y \sim z$ then $x \sim z$.

Lemma 2.4.3. Let $\sim$ be a relation on a set X by: $\forall x, y \in X$

$$x \sim y \Leftrightarrow x \cdot g = y \tag{14}$$

for some $g \in G$ where G acts on X. The relation $\sim$ is an equivalence relation.

Proof. Refer to Lemma 5.3 of [12]. □

Definition 2.4.4. [12] An equivalence class of the equivalence relation given in Lemma 2.4.3 is called an **orbit** of the action G on X. The orbit containing the element $x \in X$ is called the orbit of x under the group G denoted by $x \cdot G$.

Example 2.4.5. [12] Let G be the group $\mathbb{Z}_7^\times$, and let $X = \{1, 2, 3, 4, 5, 6\}$. In this particular example, the set X and the group G have the same elements, and so we will underline these elements when they are being treated as members of X. Consider the (right) multiplication of an element $x \in X$ by an element $g \in G$, that is, $x \cdot g$. We have $\forall x \in X, \forall g, h \in G$ where $e = 1 \in G$

$$\underline{x} \cdot e = \underline{x} \tag{15}$$

that is, the (right) multiplication of elements X by e does not alter X. Also, by associativity we have

$$\underline{x} \cdot (gh) = \underline{(x \cdot g)} \cdot h \tag{16}$$

that is, applying gh to x is the same as first applying g to x, and then applying h to the result.

Example 2.4.6. The relation of integers of congruence mod n is an equivalence relation since it satisfies the following: $\forall x, y, z \in \mathbb{Z}$

- $x \equiv x$ mod n since $x - x = 0$ and $n|0$;
- if $x \equiv y$ mod n then $y \equiv x$ mod n since if $n|(x-y)$ then $n|(y-x)$; and
- if xy mod n and $y \equiv z$ mod n then $x \equiv z$ mod n since if $n|(x-y)$ and $n|(y-z)$ then $n|(x-y+y-z) \implies n|(x-z)$.

Example 2.4.7. Take the dihedral group D_8 of a 4-sided regular polygon. Let $H =< a >$ be a subgroup of D_8 and let D_8 be a group action on the elements of itself where $D_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. The orbit of $a \in D_8$ under H is such that $a \cdot H = \{e, a, a^2, a^3\}$ and the orbit $b \cdot H = \{b, ab, a^2b, a^3b\}$. Note that these are exactly the cosets of $H \backslash D_8$.

2.5 Permutations

Definition 2.5.1. [12] Let X be a set of elements. The *permutation* σ on X is a bijection of X onto itself; $\sigma : X \to X$. For convenience we will take X to be finite where $|X| = n$, and label its elements as $X = \{1, ..., n\}$. We represent the permutations σ, $i \mapsto a_i$ $\forall i = 1, ..., n$ where $a_i \in X$, with the following matrix;

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{pmatrix} \tag{17}$$

and its inverse $\sigma^{-1}, a_i \mapsto i, \forall i = 1, ..., n$ by

$$\sigma^{-1} = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ 1 & 2 & ... & n \end{pmatrix}. \tag{18}$$

Definition 2.5.2. [12] Let σ and τ be permutations on the same set X where for $i \in X$, $(i)\sigma = a_i$ and $(i)\tau = b_i$. Since σ and τ are bijective on X, we have that the function composition, read from left to right [12], $\sigma \circ \tau : X \to X$ is bijective [13] and is given by

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{pmatrix} \begin{pmatrix} 1 & 2 & ... & n \\ b_1 & b_2 & ... & b_n \end{pmatrix} \tag{19}$$

$$= \begin{pmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & ... & a_n \\ b_{a_1} & b_{a_2} & ... & b_{a_n} \end{pmatrix} \tag{20}$$

$$= \begin{pmatrix} 1 & 2 & ... & n \\ b_{a_1} & b_{a_2} & ... & b_{a_n} \end{pmatrix}. \tag{21}$$

Definition 2.5.3. [12] We can represent a permutation using *disjoint cycle notation* which we will mostly be using. Let σ be a permutation on the finite set X and let $x \in X$. The ordered k-tuple

$$(x, (x)\sigma, (x)\sigma^2, ..., (x)\sigma^{k-1}), \tag{22}$$

where k is the smallest positive integer with the property $(x)\sigma^k = (x)(\overbrace{\sigma \circ ... \circ \sigma}^{\text{k times}}) = x$ is called the cycle of length k containing x. We then define σ with an unordered sequence of these ordered tuples, each representing a cycle in the permutation. We will omit single cycles where $(x)\sigma = x$.

Lemma 2.5.4. [12] Every permutation on a finite set can be expressed as a product of 2-cycles, also known as transpositions.

Proof. Let $\sigma \in S_n$ be a permutation on n elements. We have by Definition 2.5.3 that every cycle of the permutation can be represented by a tuple and we can check that $\sigma = (a_1, a_2, ..., a_m) = \sigma_2\sigma_3...\sigma_m = (a_1, a_2)(a_1, a_3)...(a_1, a_m)$ is the decomposition of cycles into transpositions.

We have that $\forall a \in \{1, 2, ..., n\}$

$$a\sigma = \begin{cases} a_1 & a = a_m \\ a_{i+1} & a = a_i, \forall i = 1, 2, ..., m-1. \end{cases} \tag{23}$$

For the case of the product of 2-cycles, the cycle σ_i transposes the elements a_1 and a_i therefore; when $a = a_m$ only σ_m permutes a so $a_m = a_1$ and when $a = a_i, \forall i = 1, 2, ..., m-1$, σ_i permutes a to a_1 which is then permuted by the subsequent cycle σ_{i+1} to a_{i+1} therefore $a_i = a_{i+1}$ as required. □

Definition 2.5.5. Let $\sigma \in S_n$ be a permutation on X = {1, 2, ..., n}. The *parity* of σ is said to be **even** if it can be decomposed into an even number of transpositions and **odd** otherwise.

Example 2.5.6. Let X = {1, 2, 3, 4, 5}. We define the following permutation $\sigma_1 : X \to X$ which maps $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 4$, $4, \mapsto 3$ and $5 \mapsto 5$, and $\tau_1 : X \to X$ which maps $1 \mapsto 1$, $2 \mapsto 4$, $3 \mapsto 5$, $4, \mapsto 3$ and $5 \mapsto 2$. We would then represent the permutation, $\sigma_1 \circ \tau_1$, using the following matrix;

$$\sigma_1 \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix} \tag{24}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}. \tag{25}$$

And finally, we would represent it using disjoint cycle notation as follows;

$$\sigma_1 \circ \tau_1 = (1, 2)(3, 4)(5)(1)(2, 4, 3, 5) \tag{26}$$

$$= (1, 2)(3, 4)(2, 4, 3, 5) \tag{27}$$

$$= (1, 4, 5, 2) \tag{28}$$

$$= (1, 4)(1, 5)(1, 2). \tag{29}$$

The permutation $\sigma_1 \circ \tau_1$ has odd parity.

Lemma 2.5.7. Suppose X is a set where $|X| = n$. The collection of all permutations on X, with function composition as the operation forms the symmetry group on n elements, denoted by S_n.

Proof.

- A permutation is bijective and the composition of permutations is also bijective [13] and forms another permutation, as shown in Example 2.5.6.
- It is easy to show that they are associative using steps similar to that of Definition 2.5.2, but with 3 permutations.
- The do-nothing permutation e which doesn't permute any elements of X is the identity since $e \circ \sigma = \sigma \circ e = \sigma$.
- Each permutation has an inverse as seen in Definition 2.5.1.

Therefore, S_n is a group. □

Definition 2.5.8. The alternating group A_n is a subgroup of S_n consisting of only the even permutations.

Example 2.5.9. Let $(1, 6, 4) \in S_6$, If $H =< (1, 6, 4) >$ then $H \leq A_6$.

2.6 Conjugacy

Definition 2.6.1. Let x be an element of a group G, $x \in G$. Any element of G of the form gxg^{-1} is a conjugate of x. For any subgroup $H \leq G$, $gHg^{-1} = \{ghg^{-1} : \forall h \in H\}$ is a conjugate of H.

Lemma 2.6.2. [12] Suppose σ and τ are permutations on $X = \{1, 2, ..., n\}$. The permutations σ and τ are conjugate ($\tau = \alpha^{-1}\sigma\alpha$) iff σ and τ have the same cyclic structure, in which case τ can be obtained by applying α to the symbols of σ.

Proof. Refer to Theorem 3.6 of [12]. □

Example 2.6.3. Let the set X = {1,2,3,4,5,6} and let the permutations $\sigma = (4, 3)(1, 5, 6), \alpha = (3, 2, 1)(6, 5, 4)$. The conjugate of σ is $\tau = \alpha\sigma\alpha^{-1} = (1, 2, 3)(4, 5, 6)(4, 3)(1, 5, 6)(3, 2, 1)(6, 5, 4) = (2, 6)(3, 4, 5)$. This is equivalent to $\tau = (4\alpha, 3\alpha)(1\alpha, 5\alpha, 6\alpha) = (2, 6)(3, 4, 5)$.

2.7 Homomorphisms

Definition 2.7.1. [12] Let $(G_1, \circ)$ and $(G_2, \star)$ be groups and let ϕ be a map from G_1 to G_2. The map ϕ is called a homomorphism from G_1 to G_2 if, $\forall g, h \in G_1$,

$$(g \circ h)\phi = g\phi \star h\phi. \tag{30}$$

Definition 2.7.2. Let ϕ be a homomorphism from G_1 to G_2. ϕ is called the *trivial homomorphism* if $a\phi = e \ \forall a \in G_1$.

Definition 2.7.3. Let ϕ be a homomorphism from G_1 to G_2. ϕ is called an *isomorphism* if it is also a bijection from G_1 to G_2; the groups G_1 and G_2 are said to be isomorphic, and we denote it by $G_1 \cong G_2$.

Definition 2.7.4. Let ϕ be a homomorphism. It is called an automorphism if it is an isomorphism of G_1 to itself.

Lemma 2.7.5. [12] Let G and H be groups with identities e_G and e_H respectively and let $\phi : G \to H$ be a homomorphism. Then, $ker(\phi) \leq G$.

Proof. Refer to [7] page 30 Theorem 9.8. □

Corollary 2.7.6. Let G and H be groups with identities e_G and e_H respectively and let $\phi : G \to H$ be a homomorphism. Then, $ker(\phi) \trianglelefteq G$.

Proof. It follows from Lemma 2.7.5 that $ker(\phi) \leq G$. Let $i \in ker(\phi)$ and $g \in G$. Then

$$(gag^{-1})\phi = g\phi a\phi g^{-1}\phi = g\phi 1_H g^{-1}\phi = g\phi g^{-1}\phi = (gg^{-1})\phi = 1_G\phi = 1_H \tag{31}$$

Therefore, $(gag^{-1})\phi \in ker(\phi)$ and so $ker(\phi) \trianglelefteq G$. □

Lemma 2.7.7. Let G be a group. $G \cong \{e\} \times G \cong G \times \{e\}$.

Proof. Trivial. □

Example 2.7.8. Let $\phi : S_n \to \mathbb{Z}_2^+$ such that $\forall \sigma \in S_n$,

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation,} \\ 1 & \text{if } \sigma \text{ is an odd permutation,} \end{cases} \tag{32}$$

The mapping ϕ is a homomorphism.

Proof. $\forall \sigma, \tau \in S_n$ if σ is odd and τ is even or vice versa, $\sigma \circ \tau$ is odd. If both σ and τ are even or odd permutations then $\sigma \circ \tau$ is even. It follows that when σ is odd and τ is even or vice versa,

$$(\sigma \circ \tau)\phi = 1 \tag{33}$$
$$= \sigma\phi + \tau\phi \tag{34}$$
$$= 1 + 0 \text{ OR } 0 + 1 \bmod 2 \tag{35}$$
$$= 1 \bmod 2; \tag{36}$$

when both σ and τ are even or odd permutations,

$$(\sigma \circ \tau)\phi = 0 \tag{37}$$
$$= \sigma\phi + \tau\phi \tag{38}$$
$$= 0 + 0 \text{ OR } 1 + 1 \bmod 2 \tag{39}$$
$$= 0 \bmod 2. \tag{40}$$

Therefore ϕ is a homomorphism. □

Example 2.7.9. Let $G = \mathbb{Z}_8$ and $H = \{0, 4\}$ be a subgroup of G. We say $H \cong \mathbb{Z}_2$.

Proof. We define the mapping $\phi : H \to \mathbb{Z}_2$ where $0 \mapsto 0$ and $4 \mapsto 1$.

$$(0 + 0)\phi = 0\phi + 0\phi = 0 + 0 = 0 \tag{41}$$
$$(0 + 4)\phi = 4\phi = 1 = 0 + 1 = 0\phi + 4\phi \tag{42}$$
$$(4 + 0)\phi = 4\phi = 1 = 1 + 0 = 4\phi + 0\phi \tag{43}$$
$$(4 + 4)\phi == 0\phi = 0 = 1 + 1 = 4\phi + 4\phi. \tag{44}$$

We note that addition before the mapping is modulo 8 and after the mapping is modulo 2. □

2.8 Direct & Semi-direct Products

Definition 2.8.1. [12] Let $G_1, G_2, ..., G_n$ be groups and let

$$G = \prod_i^n G_i = G_1 \times G_2 \times ... \times G_n = \{(a_1, a_2, ..., a_n) : a_i \in G_i, 1 \leq i \leq n\}$$

be the Cartesian product, then G is a group with respect to the binary operation

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) := (a_1 b_1, a_2 b_2, ..., a_n b_n).$$

The identity element is $e = (e_1, e_2, ..., e_n)$ and the inverse $(a_1, a_2, ..., a_n)^{-1} = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$. We call G the **direct product** of $G_1, G_2, ..., G_n$

Proof. Closure and associativity hold by the individual group operations. $\forall a_i \in G_i, (a_1, a_2, ..., a_n)(e_1, e_2, ..., e_n) = (e_1, e_2, ..., e_n)(a_1, a_2, ..., a_n) = (a_1 e_1, a_2 e_2, ..., a_n e_n) = (e_1 a_1, e_2 a_2, ..., e_n a_n) = (a_1, a_2, ..., a_n)$ and so e $= (e_1, e_2, ..., e_n)$ is in fact the identity. $(a_1, a_2, ..., a_n)(a_1^{-1}, a_2^{-1}, ..., a_n^{-1}) = (a_1 a_1^{-1}, a_2 a_2^{-1}, ..., a_n a_n^{-1}) = (e_1, e_2, ..., e_n)$ and so $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$ is indeed the inverse. Therefore the direct product is a group. □

Definition 2.8.2. [12] Let $K \leq G$. The subgroup K is called *normal* in G, denoted by $K \trianglelefteq G$ iff $\forall g \in G$

$$gK = Kg \tag{45}$$

Theorem 2.8.3. *[12] If $K \leq G$, then the following conditions are equivalent:*

1. $K \trianglelefteq G$;
2. $\forall g \in G\ g^{-1}Kg \subseteq K$;
3. $\forall g \in G$ *and* $\forall k \in K$, $g^{-1}kg \in K$.

Proof. Refer to [12] page 31. □

Definition 2.8.4. [12] Let G be a group with a subgroup K and normal subgroup H such that

$$G = AK \text{ and } A \cap K = \{e\}. \tag{46}$$

In this case, G is called a semi-direct product of H by K and we write

$$G \cong K \rtimes H. \tag{47}$$

Example 2.8.5. Let $G = \mathbb{Z}_3 \times \mathbb{Z}_4$. By Defnition 2.8.1 the identity e $= (0, 0)$ and $\forall a_1 \in \mathbb{Z}_3$ and $a_2 \in \mathbb{Z}_4$ the inverse of $(a_1, a_2) = (a_1^{-1}, a_2^{-1})$ which can be found applying the Euclidean Algorithm [12].

Example 2.8.6. Let $G = D_8$ and the subgroups $H =< a >$ and $K =< b >$. We have that $a \in G$, $aH = H = Ha$ and $bH = \{b, ab, a^2b, a^3b\} = Hb$ therefore $H \trianglelefteq G$. We also have that HK $= \{\text{hk} : \forall h \in H, \forall k \in K\} = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\} = G$ and $H \cap K = e$. Therefore $D_8 \cong < b > \rtimes < a >$.

Part I
The 3D Cubes

In this paper, we will be focusing on the structure of two very famous cubes invented by Erno Rubik; the Pocket Cube and the Rubik's Cube. The rules and goals of these puzzles are identical with the differences in difficulty and structure stemming only from the size of the puzzle. In this section we will define the rules and goals of such puzzles and build their respective group structure. All Definitions, Propositions and Theorems in this section are generalised for both of the 3D cubes unless otherwise specified.

3 Overview

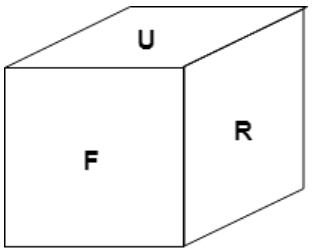

Figure 1: Face labels for the Cubes.

The Pocket and Rubik's Cubes are 3-Dimensional puzzles. The cubes have 6 faces. When a cube is held in front of us, we label the faces as follows; "**Up**" for the face facing up, "**Down**" for the face facing down, "**Front**" for the face facing us, "**Back**" for the face facing away from us, "**Right**" for the face facing to the right of us and "**Left**" for the one facing to the left. For simplicity we sometimes use the first letter to denote the face, as seen in Figure 1.

A cube consists of cubies [7] (depicted in Figures 2 and 4) held together by a central core, whose mechanism allows the cubies of the cube to slide over each other by rotating the cubies of a face. We will, however, imagine that the cubies are placed in an invisible mesh of placeholders called cubicles [7]. There are 3 types of cubies, each with a corresponding type of cubicle, that are considered in the Pocket and Rubik's cubes; the corner, edge and center cubies. Each cubie has coloured facets [6]. The corner cubies have 3, edge cubies have 2 and center cubies have only 1 coloured facets; this is visualised in Figures 2 and 4.

The components which make up the Pocket Cube and Rubik's Cube are different due to the size of the puzzle (the number of moving parts), and so we will describe them separately.

Pocket Cube

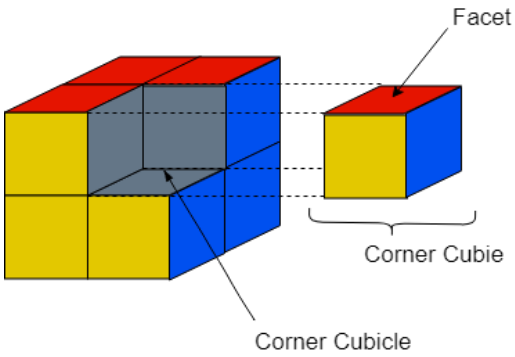

Figure 2: (a) Labelled Components of the Cube

The Pocket Cube is made up of 8 corner cubies where each cubie can be in 8 possible cubicles; as seen in Figure 2. Once a cubicle is occupied by a cubie, another cubie may not occupy the same cubicle. Therefore, there are $8! = 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 4.0320 \times 10^4$ permutations of, or possible ways to arrange, the cubies.

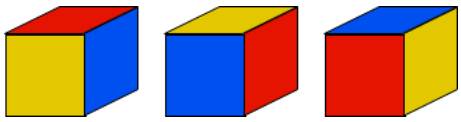

Figure 3: Possible orientations of a corner cubie

Each corner cubie has 3 facets, each with a different fixed colour (we are not allowed to remove or change the coloured stickers on the facets) so each cubie has 3 possible ways of being oriented within a cubicle; as seen in Figure 3. By combining the possible permutations and orientations of the cubies in the cubicles, we find that there are $8! \times 3^8 = \mathbf{2.64539520 \times 10^8}$ possible *configurations*, or arrangements, of the cubies of the Pocket Cube. These configurations make up the set $C_{\mathcal{P}}$ of all possible configurations of the Pocket Cube. However, not all of these are valid configurations of the Pocket Cube because a valid configuration can only be obtained by adhering to the rules of the puzzle.

Rubik's Cube

The Rubik's Cube is made up of 8 corner cubies, 12 edge cubies and 6 center cubies where each type of cubie has a corresponding cubicle; as seen in Figure 4. We note here that the center cubies are fixed in their cubicles. Once a cubicle is occupied by a cubie, another cubie may not occupy the same cubicle. Therefore, there are $8! \times 12! = 1.9313345 \times 10^{13}$ permutations of the cubies.

As in the case of the Pocket Cube, the corner cubies have 3 orientations, whereas the edge cubies only have 2 as seen in Figure 5. By considering the permutations and orientation, there are $8! \times 3^8 \times 12! \times 2^{12} = \mathbf{5.1902404 \times 10^{20}}$ possible configurations of the cubies. These configurations make up the set $C_{\mathcal{R}}$ of all configurations of the Rubik's Cube. However, not all of these are valid configurations of the Pocket Cube because, as before, a valid configuration can only be obtained by adhering to the rules of the puzzle which we will define in the next section.

Definition 3.0.1. A *configuration* of a 3D Cube represents the positions and orientation of each of the cubies in regards to the cubicles. A cube is in a *solved configuration*, denoted by $i \in C$ when each of the faces of the cube is coloured with a single colour. We will formalise this further in Section 4.

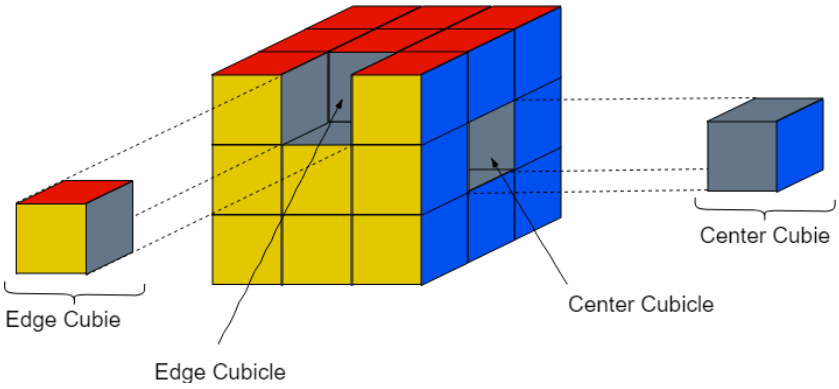

Figure 4: (b) Labelled Components of the Cube

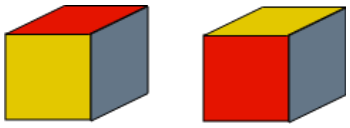

Figure 5: Possible orientations of an edge cubie

Notation:

- When defining variables specifically for the Pocket Cube or Rubik's Cube we will denote this by adding the subscript $\mathcal{P}$ or $\mathcal{R}$ respectively, to avoid ambiguity.
- For the remainder of this paper, a configuration $c \in C$ is defined such that c is an unordered tuple that holds, separately, the position and orientation of each type of cubie. Therefore, in the case of the Pocket Cube, $\forall p \in C_{\mathcal{P}}$, $p = (p_\sigma, p_{\mathbf{x}})$, and, in the case of the Rubik's Cube, $\forall r \in C_{\mathcal{R}}$, $r = (r_\sigma, r_\tau, r_{\mathbf{x}}, r_{\mathbf{y}})$. The subscripts σ and τ denote the positions of the corner and edge cubies respectively, and the subscripts $\mathbf{x}$ and $\mathbf{y}$ denote their orientations respectively.

3.1 Rules of the 3D Cubes

Upon examination of each individual cubie of the cubes, we observe that the colours of the facets of a cubies are such that the colours of the facets are unique and no single cubie contains the following pairs of colours; (white, yellow), (blue, green) or (orange, red). This implies that these pairs of colours are never adjacent to each other and defines the ***adjacency*** of the colours rule of a cube.

Definition 3.1.1. *Adjacency* of the colours of a 3D Cube are such that the following pairs of colours must not be adjacent to each other; (white, yellow), (blue, green) and (orange, red).

The ultimate goal of the puzzle is to arrange the cubies in such a way that each of the 6 faces of the cube is coloured with a single colour, and it follows that the adjacency of colours must hold. We define this arrangement, or configuration, as the ***solved configuration*** of the Cube.

We could quite simply 'solve' the puzzle by dismantling the cube into it's individual components and reassembling it to a solved configuration. However, one of the rules of the puzzle is that the solved configuration must be attained using a combination of the ***basic moves***.

Definition 3.1.2. A *basic move* is defined as a 90° clockwise rotation of a face (as if you were facing it) and its corresponding inverse as a 90° anti-clockwise rotation. There are 6 basic moves which are denoted **U, D, F, B, R** and **L** (using Singmaster Notation [1]) for each **Up, Down, Front, Back, Right** and **Left** face respectively. The inverses will be denoted with a superscript as either $\mathbf{U}^{-1}$ or $\mathbf{U}'$. We have that repeating a basic move 3 times, take $\mathbf{U}^3$ which is a 270° clockwise rotation of the "**Up**" face, is the same as the inverse of that basic move, $\mathbf{U}^{-1}$ a 90° anti-clockwise rotation of the same face. Repeating a

basic move 4 times, take $\mathbf{U}^4$ which is a 360° rotation of the **Up** face, is the same as not doing a move at all, denoted by e. We will denote the moves U^3 or F^2, for example, as **U3** and **F2** respectively when counting them as 1 move [20]. We denote the set of basic moves by $\mathcal{B}$.

When talking about move sequences of the cube, we have two commonly accepted ways to count the number of moves in a sequence; using the half-turn or quarter-turn metric [20]. For convenience, we will define the set of basic moves $\mathcal{B}$ as the set of moves which count as a single move.

Quarter-Turn Metric

$$\mathcal{B} = \{\mathbf{U1}, \mathbf{U3}, \mathbf{D1}, \mathbf{D3}, \mathbf{F1}, \mathbf{F3}, \mathbf{B1}, \mathbf{B3}, \mathbf{R1}, \mathbf{R3}, \mathbf{L1}, \mathbf{L3}\} \tag{48}$$

Half-Turn Metric

$$\mathcal{B} = \{\mathbf{U1}, \mathbf{U2}, \mathbf{U3}, \mathbf{D1}, \mathbf{D2}, \mathbf{D3}, \mathbf{F1}, \mathbf{F2}, \mathbf{F3}, \mathbf{B1}, \mathbf{B2}, \mathbf{B3}, \mathbf{R1}, \mathbf{R2}, \mathbf{R3}, \mathbf{L1}, \mathbf{L2}, \mathbf{L3}\} \tag{49}$$

If we take a cube and put it in a solved configuration, applying a basic move to it will scramble it. If we continue to apply basic moves it will take the cube to another scrambled position (unlikely, but possibly the solved configuration). These possible sequence of moves make up the set of all valid moves of the cube. We will sometimes find that two unique sequence of basic moves m_1, m_2 when applied to a solved configuration arrive at the same configuration; in this case we say the moves are equal, $m_1 = m_2$, and we would prefer to use the shorter sequence of basic moves. We note that these collisions are different for the Pocket Cube and Rubik's Cube.

Definition 3.1.3. A *valid move* is some unique combination of the basic moves. We denote the generic set of all valid moves by $\mathcal{G}$. We represent a valid move $m \in \mathcal{G}$ as a sequence of basic moves $m = b_1 b_2 ... b_n$ where $b_i \in \mathcal{B}$ and $n \in \mathbb{N}$ is the length, or count, of the valid move. We have a special case, when $n = 0$, which is the do nothing move, represented by the empty sequence e.

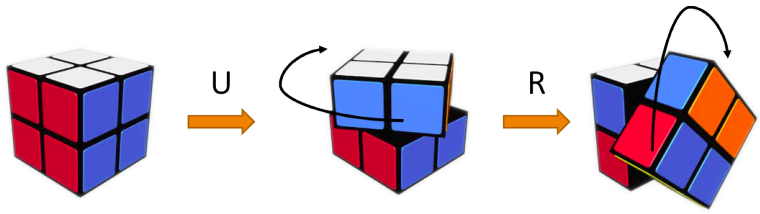

Figure 6: The order of applying move **UR**
Source: Screen-shots of these Pocket Cubes were taken from [22].

Example 3.1.4. For $m \in \mathcal{G}$ where m = **UR**, we apply **U** followed by **R** to the current configuration of the cube as seen in Figure 6.

Example 3.1.5. For $m_1 \in \mathcal{G}$ where m = **F**, $m_2 = \mathbf{U^4F} \in \mathcal{G}$ is a collision since $\mathbf{U}^4 = e$ means that $m_2 = e\mathbf{F} = \mathbf{F} = m_1$.

Definition 3.1.6. A *valid configuration* is one that can be achieved from another valid configuration using only a valid move. We denote the set of all valid configurations as V.

Definition 3.1.7. A solved configuration is a valid configuration.

In 1995, the mathematician Michael Reid proved that the configuration of the Rubik's cube called the "Superflip" required at the very least 20 basic moves [4], using the half-turn metric, to get to from the solved configuration. The configuration is such that all the cubies are correctly positioned, all the corner cubies are correctly oriented, however, the edge cubies are all incorrectly oriented, or "flipped", as seen in Figure 7.

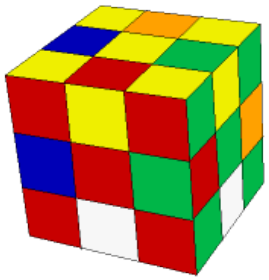

Figure 7: The "Superflip" Position

Example 3.1.8. Starting from a solved configuration of a Rubik's Cube, the move $m \in \mathcal{R}$ of length 20, using the half-turn metric, called the superflip, is the sequence

$$m = \mathbf{U1R2F1B1R1B2R1U2L1B2R1U3D3R2F1R3L1B2U2F2} \tag{50}$$

which takes the Rubik's Cube to the valid configuration in Figure 7.

3.2 The Cube Group

We can make the set of all valid moves of a 3D Cube into a **group** $(\mathcal{G}, \circ)$, sometimes denoted as just $\mathcal{G}$. The elements of $\mathcal{G}$ are all the possible valid moves of the cube, which are the basic moves and every unique combination of them by the **Cube Group operation**.

Definition 3.2.1. [7] The *Cube Group operation* is the binary operation, $\circ$, such that, $\forall m_1, m_2 \in \mathcal{G}, m_1 \circ m_2$, sometimes denoted as $m_1 m_2$, is the move where we first do m_1 then m_2.

Theorem 3.2.2. *The set of all valid moves of a 3D Cube is a group under the Cube Group operation.*

Proof. $\forall a, b, c \in \mathcal{B}$ and $\forall i, j, k \in \mathbb{N}_0$

- We have that $\forall m_1, m_2 \in \mathcal{G}$, m_1 and m_2 are sequence of basic moves; $m_1 = a_1 a_2 ... a_i$ and $m_2 = b_1 b_2 ... b_j$; and we have that $m_1 \circ m_2$ is the move where we first apply the sequence of moves of m_1 followed by the sequence of moves of m_2. This is effectively applying the sequence of moves concatenated together and so $m_1 \circ m_2 = a_1 a_2 ... a_i b_1 b_2 ... b_j$ which is a sequence of basic moves. Therefore the moves are *closed* under the group operation.
- Let $m_1 = b_1 b_2 ... b_j \in \mathcal{G}$. If we apply the same sequence of moves as m_1, but in reverse order and with each of the basic moves replaced with their corresponding inverses (defined in Definition 3.1.2), we get a move $m_2 \in \mathcal{G}$ such that $m_2 = b_j^{-1} b_{j-1}^{-1} ... b_1^{-1}$, which effectively undoes m_1. We now have that $m_1 \circ m_2 = e$ and so $m_2 = m_1^{-1}$. Therefore $\forall m \in \mathcal{G}$ there exists a right inverse m^{-1}.
- We have that e is the empty sequence of moves, the do nothing move. e is a member of $\mathcal{G}$ since it is equivalent to doing any basic move 4 times. $\forall m \in \mathcal{G}$ we have that doing the empty sequence of moves then the sequence of moves $m = b_1, b_2 ... b_j$ is the same as doing the sequence of moves m followed by the empty sequence, which is also the same as just doing the sequence of moves m. We have that $e \circ m = b_1, b_2 ... b_j = m \circ e = m$, therefore, $e \in \mathcal{G}$ is the *identity*.
- $\forall m_1, m_2, m_3 \in \mathcal{G}$ where $m_1 = a_1 a_2 ... a_i, m_2 = b_1 b_2 ... b_j$ and $m_3 = c_1 c_2 ... c_k$. We see that

$$\begin{aligned} m_1 \circ (m_2 \circ m_3) &= (a_1 a_2 ... a_i) \circ (b_1 b_2 ... b_j c_1 c_1 ... c_k) \\ &= a_1 a_2 ... a_i b_1 b_2 ... b_j c_1 c_2 ... c_k \\ &= (a_1 a_2 ... a_i b_1 b_2 ... b_j) \circ (c_1 c_2 ... c_k) \\ &= (m_1 \circ m_2) \circ m_3 \end{aligned}$$

Therefore the group operation is *associative*. □

By Theorem 3.2.2, $\mathcal{G}$ is a group. This is generic for both the Pocket Cube and Rubik's Cube where we denote their groups as $\mathcal{P}$ and $\mathcal{R}$ respectively. From here we can very easily describe the Cube Group $\mathcal{G}$, whose elements are made up of a sequence of basic moves (refer to Definition 3.1.3), as the elements generated by the set of basic moves $\mathcal{B} = \{\mathbf{U,D,F,B,R,L}\}$. Therefore, $\mathcal{G} =< \mathbf{U,D,F,B,R,L} >$.

It is easy to see that these groups have subgroups, some of which are trivial, some of which are obvious, however, there are some which exhibit interesting properties such as the *2-generator* subgroup of the Pocket Cube Group (refer to [9] for more details).

Example 3.2.3. Let $\mathcal{P}$ be the Pocket Group. $I = \{e\}$ is the trivial subgroup of $\mathcal{P}$. Take the subset $H = \{e, \mathbf{U}, \mathbf{U}^2, \mathbf{U}^3\}$ of $\mathcal{P}$. H is *closed* under the cube group operation since $\mathbf{U}^4 = e$ means that every combination of the elements in H which are not in H can be simplified to be a member of H. The group is *associative* by the Pocket Group operation and has the *identity* e. It contains *inverses* for each element such that $\mathbf{U}\mathbf{U}^3 = \mathbf{U}^2\mathbf{U}^2 = e$. Therefore $H \leq \mathcal{P}$.

We can generalise the subgroup H in Example 3.2.3 to be the set of subgroups $\{H_b : b \in \mathcal{B}\}$ where

$$H_b =< b : b^4 = e > . \tag{51}$$

The generator relations (see Definition 2.2.7) of the subgroup defines the structure of the group. In this case there is only 1 and in the case of the dihedral groups (see example 2.2.8) there are 3. These generator relations make understanding the group structure and how it behaves much simpler. Therefore, in the case of the Cube Group, we have that

$$\mathcal{G} =< \mathbf{U,D,F,B,R,L} : R > \tag{52}$$

where $\mathbf{U^4}, \mathbf{D^4}, \mathbf{F^4}, \mathbf{B^4}, \mathbf{R^4}, \mathbf{L^4} \in R$.

The problem is that it is difficult to show what these generator relations are and, even so, there would be too many understand the group (refer to [10] page 35-40 for examples and analysis), assuming that it is even possible to find the set of independent generators relations.

Other than a few basic ones which are common amongst the 3D cubes, the set of independent generator relations for the Pocket Cube and Rubik's cube are different.

Proposition 3.2.4. $R_{\mathcal{P}} \neq R_{\mathcal{R}}$.

Proof. Let $m = \mathbf{LR^1U^2L^1RB^2}$. In the Pocket Group, $m = e$ and so $m \in R_{\mathcal{P}}$ however in the Rubik's Group m cycles the positions of 3 edge cubies and so $m \notin R_{\mathcal{R}}$. □

3.3 The Cube Group and The Configurations

W have shown that the Cube Group represents the valid moves of a 3D Cube, however, how does a move of this group affect the configuration of the cube? How does the Cube Group relate to the configurations of the cube? It is easy to see that there is a relationship, if we begin in a solved configuration and apply a valid move, for example $\mathbf{U}$, then the cube is no longer in a solved configuration, but in another valid configuration (Definition 3.1.6). We can formalise this using group actions where we say that a valid move acts on a configuration giving us another configuration in the same orbit.

Theorem 3.3.1. *The Cube Group, $\mathcal{G}$, acts on the set of configurations of the cube (allowing both valid and invalid configurations), C, by the right group action such that $\forall c \in C, \forall g \in \mathcal{G}$*

$$\phi : C \times \mathcal{G} \to C \tag{53}$$

$$(c, g) \mapsto c \cdot g. \tag{54}$$

Proof. Suppose $\mathcal{G}$ acts on C by $(c, g) \mapsto c \cdot g$. The identity move $e \in \mathcal{G}$ is the move which applies no basic moves to the configuration, the do nothing move. This means that $\forall c \in C, c \cdot e = c$, as required. $\forall g, h \in \mathcal{G}$, we have that $g \circ h$ is the move which applies move g followed by move h to the current configuration c, $\forall c \in C$. Therefore, $c \cdot (g \circ h) = (c \cdot g) \cdot h$ and the theorem holds. □

And so, we have that the Cube Group $\mathcal{G}$ acts on the set of all configurations C whose orbit containing the solved configuration (or any other valid configuration) is the set of all valid configurations V.

By Definition 2.4.4, the orbit of the solved configuration i under $\mathcal{G}$ is the equivalence class $i \cdot \mathcal{G}$ such that $\forall c \in C$ and $\forall g \in \mathcal{G}$,

$$i \sim c \Leftrightarrow i \cdot g = c. \tag{55}$$

Intuitively, this makes sense because a valid configuration is one that is obtained from another valid configuration by a valid move which eventually arrives at the solved configuration.

In the next section, we will formalise and understand the orbits of this group action and give a formal definition for the set of valid configurations of the Pocket Cube and Rubik's Cube.

4 Valid Configurations of the 3D Cubes

The Pocket Cube is the simplest of Erno Rubik's 3D cubes and contains only 8 corner cubes. The 3x3x3 Rubik's Cube also has 8 corner cubies and, interestingly, this is the case for all $n \times n \times n$ Rubik's Cubes; with the added complexity coming from the edge and center cubies. We will see in the case of the Rubik's Cube that it's group structure, if we were to ignore the edge and center cubies, is that of the Pocket Cube. This can be generalised for all 3D cubes of this kind. At the end of the section we will describe this intuitively and mathematically for the Rubik's Cube.

If we assume that we are able to freely permute and re-orient each cubie using a combination of the basic moves, implying there exists a move which can permute any 2 edge or corner cubies and a move which can rotate a single cubie without affecting the other cubies, then we are done and there are 2.64539520×10^8 and 5.1902404×10^{20} valid configurations in $V_{\mathcal{P}}$ and $V_{\mathcal{R}}$ for the Pocket and Rubik's Cube respectively. This implies that there is only one orbit of the Cube Group action on their respective set of all possible configurations, $C_{\mathcal{P}}$ and $C_{\mathcal{R}}$, and so, $V_{\mathcal{P}} = C_{\mathcal{P}}$ and $V_{\mathcal{R}} = C_{\mathcal{R}}$. However, we first need to prove/disprove these assumptions, and to do that we need to define a move as a permutation and re-orientation of the cubies.

The affect that a move has on the Pocket Cube and Rubik's Cube is different due to the additional complexity of the Rubik's Cube. Therefore, in this section we will cater to them separately.

4.1 The Pocket Cube

4.1.1 Permutation of the Cubies

In order to consider only the permutations, we have to ignore the orientation of the cubies and have that a move is some permutation of the cubies, in this case, the 8 corner cubies.

Since, we only care about the permutations of the cubies - the position in terms of which cubicle a cubie is in and which cubicle it is moved to after applying a move - we label the cubicles using Janet's notation [7] and, equivalently, index them using the numbers 0 to 7 [1] as seen in Figure 8, where the non-indexed 0^{th} cubicle is the dbl cubicle.

We can now define each of the 6 basic moves as the following permutations;

$$\mathbf{U}_\sigma = (\text{ubl, ubr, ufr, ufl}) = (4, 5, 6, 7) \tag{56}$$
$$\mathbf{D}_\sigma = (\text{dbl, dfl, dfr, dbr}) = (0, 1, 2, 3) \tag{57}$$
$$\mathbf{F}_\sigma = (\text{dfl, ufl, ufr, dfr}) = (1, 7, 6, 2) \tag{58}$$
$$\mathbf{B}_\sigma = (\text{dbl, dbr, ubr, ubl}) = (0, 3, 5, 4) \tag{59}$$
$$\mathbf{R}_\sigma = (\text{ufr, ubr, dbr, dfr}) = (2, 6, 5, 3) \tag{60}$$
$$\mathbf{L}_\sigma = (\text{dbl, ubl, ufl, dfl}) = (0, 4, 7, 1). \tag{61}$$

This means that the permutation of the corner cubies by a valid move m, denoted by m_σ, belongs to the symmetric group on 8 elements, S_8. We now have that just the cubie permutations of the valid

[1] We index the cubies from 0 to 7 instead of 1 to 8 for later convenience.

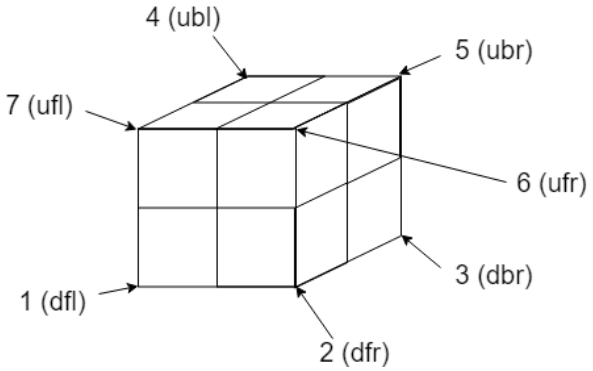

Figure 8: Indexing of the corner cubicles.

moves form the subgroup $\mathcal{P}_\sigma =< \mathbf{U}_\sigma, \mathbf{D}_\sigma, \mathbf{F}_\sigma, \mathbf{B}_\sigma, \mathbf{R}_\sigma, \mathbf{L}_\sigma >$ of S_8. We can easily verify that Theorem 3.2.2 still holds.

Lemma 4.1.1. There exists a move in $\mathcal{P}_\sigma$ which permutes any 2 cubies.

Proof. Let $m_0 \in \mathcal{P}_\sigma$ be the move such that $m_0 = \mathbf{R^{-1}FURU^2RFR^2FUF} =$ (dfl, ufl). We can conjugate m_0 with any move m to get $m^{-1}m_0m =$ (dfl m, ufl m) where $m \in \mathcal{P}_\sigma$ is the move which sends cubie dfl to cubie C_1 and cubie ufl to cubie C_2. Therefore $m^{-1}m_0m = (C_1, C_2)$ (refer to [7] for the full list of moves that proves the existence of all the transpositions). Note that, though not necessary, this move doesn't affect the orientations. □

Lemma 4.1.2. The permutations of the corner cubies by the valid moves, $\mathcal{P}_\sigma$, is the group S_8.

Proof. We have that $\mathcal{P}_\sigma =< \mathbf{U}_\sigma, \mathbf{D}_\sigma, \mathbf{F}_\sigma, \mathbf{B}_\sigma, \mathbf{R}_\sigma, \mathbf{L}_\sigma >$, therefore, $\mathcal{P}_\sigma$ is generated by elements of S_8 and so by Definition 2.2.3, $\mathcal{P}_\sigma \leq S_8$. By Lemma 4.1.1 the group $\mathcal{P}_\sigma$ contains the permutations which transpose any two cubies, therefore, by Lemma 2.5.4, any permutation in S_8 can be generated by these moves and so $S_8 \leq \mathcal{P}_\sigma$. Finally, since $\mathcal{P}_\sigma \leq S_8$ and $S_8 \leq \mathcal{P}_\sigma$, we have that $\mathcal{P}_\sigma = S_8$. □

We have now verified our first assumption that we are able to freely permute the cubies since $\mathcal{P}_\sigma = S_8$. Therefore the orbit of the solved configuration i under $\mathcal{P}_\sigma$ is the set of valid permutations of the cubies V_σ, which is also the set of all permutations of the cubies. Therefore $V_\sigma = C_\sigma$.

4.1.2 Orientation of the Cubies

Firstly, we need to define some notation for the orientation of the corner cubies. We start by looking at the cube in the solved configuration (WLOG we choose one solved configuration and ignore the others); in this configuration we know that each cubie is correctly positioned and, more importantly, correctly oriented. There are 8 cubies each of which can be oriented in 3 different ways, the correct one being its orientation in the solved configuration. When not in the solved configuration we can define its orientation as the number of clockwise turns away from its correct orientation (as done by Janet Chen in [7]). We have that being 3 clockwise turns away from its correct orientation is equivalent to the correct orientation and so we can model this behaviour using the additive group of integers modulo 3, $\mathbb{Z}_3$.

The orientation of each cubie in any given state can be denoted using $x_i \in \mathbb{Z}_3, \forall i = 0, 1, ..., 7$. We begin by labelling the facet of each cubie which is in either the **Up** or **Down** face (it's easy to see that a single cubie can't have facets in both) with x_i where i is the index of the cubie as defined in Figure 8. While moving clockwise about the cubie, we label the next facet $x_i + 1$ and then the subsequent one $x_i + 2$, which is depicted in Figure 9.

Definition 4.1.3. The orientation of the corner cubies is represented by the tuple $\mathbf{x} = (x_0, x_1, ..., x_7), x_i \in \mathbb{Z}_3$ and in a solved configuration, $x_i = 0, \forall i = 0, 1, ..., 7$.

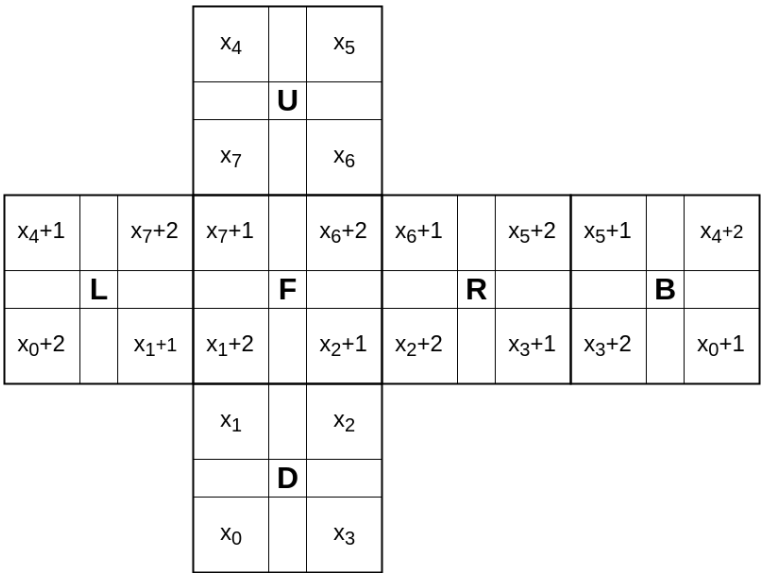

Figure 9: Labelled orientation of the corner cubies

We now have a way to represent the orientations of each corner cubie. By starting from an arbitrary orientation of the cube, $\mathbf{x} = (x_0, x_1, ..., x_7)$, we get the orientations of the cube in Table 1 after applying each of the basic moves.

Move	**Orientation, $\vec{x'}$, after applying a move**
$\mathbf{U_x}$	$(x_0, x_1, x_2, x_3, x_7, x_4, x_5, x_6)$
$\mathbf{D_x}$	$(x_3, x_0, x_1, x_2, x_4, x_5, x_6, x_7)$
$\mathbf{F_x}$	$(x_0, x_2 + 2, x_6 + 1, x_3, x_4, x_5, x_7 + 2, x_1 + 1)$
$\mathbf{B_x}$	$(x_4 + 1, x_1, x_2, x_0 + 2, x_5 + 2, x_3 + 1, x_6, x_7)$
$\mathbf{R_x}$	$(x_0, x_1, x_3 + 2, x_5 + 1, x_4, x_6 + 2, x_2 + 1, x_7)$
$\mathbf{L_x}$	$(x_1 + 2, x_7 + 1, x_2, x_3, x_0 + 1, x_5, x_6, x_4 + 2)$

Table 1: Re-orientations of the corner cubies by the basic moves

If we continue to assume that we can freely re-orient the cubies, then the change in orientation of the cubies can be represented by the group $(\mathbb{Z}_3)^8$, however, this is not the case.

Proposition 4.1.4. If $m \in \mathcal{P}$, a valid move, then $\sum x_i \equiv \sum x'_i \mod 3$ where $\vec{x'}$ is the orientation of the corner cubies after applying the move m.

Proof. We take the orientation of the cubies to be the tuple $\mathbf{x} \in (\mathbb{Z}_3)^8$ where $\sum x_i \equiv a \mod 3 \, \forall i = 0, ..., 7$. Upon applying each of the moves, we get the orientations in Table 1.

It follows that for the case after move **U** or **D**, $\sum x'_i = \sum x_i \equiv a \mod 3$, and, also, for the case after moves **F**, **B**, **R** or **L**, $\sum x'_i = \sum x_i + 6 \equiv a \mod 3$.

□

We have now shown that not all possible orientations of the corner cubies are considered valid and so there isn't a move that rotates a cubie without affecting the other cubies, effectively disproving our second assumption. We now have that the re-orientations of the cubies preserve the $\sum_{i=0}^{7} x_i$ which is equivalent to freely choosing the orientation of 7 cubies, since the last one is set to preserve $\sum_{i=0}^{7} x_i$.

Therefore, the group which represents the valid re-orientation of the corner cubies is $\mathcal{P}_\mathbf{x} = (\mathbb{Z}_3)^7$ whose orbit under the orientation of the cubies in a solved configuration $i_\mathbf{x}$ forms the set of valid orientations of the Pocket Cube, $V_\mathbf{x}$.

Lemma 4.1.5. If $\mathbf{x} \in V_{\mathbf{x}}$ then $\sum_{i=0}^{7} x_i \equiv 0 \bmod 3$.

Proof. It follows from Section 3.3 and Proposition 4.1.4 that $V_{\mathbf{x}} = i_{\mathbf{x}} \cdot \mathcal{P}_{\mathbf{x}}$ where $i_{\mathbf{x}} = \mathbf{0}$ and since every valid move preserves the sum, we have that $\forall \mathbf{x} \in V_{\mathbf{x}}, \sum_{i=0}^{7} x_i \equiv \sum_{i=0}^{7} v_i \equiv 0 \bmod 3$. □

Since $\sum_{i=0}^{7} x_i \equiv a \bmod 3$ where $\mathbf{x} \in C_{\mathbf{x}}$ and the action of $\mathcal{P}_{\mathbf{x}}$ on the set of all possible orientations of the cubies $C_{\mathbf{x}}$ preserves $\sum_{i=0}^{7} x_i$, we have that there are 2 other orbits. These are the cases where $a = 1$, which is the orbit of (0,0,0,0,0,0,0,1) under $\mathcal{P}_{\mathbf{x}}$, or $a = 2$, which is the orbit of (0,0,0,0,0,0,0,2) under $\mathcal{P}_{\mathbf{x}}$; and these orbits represent 2 different sets of invalid orientations.

4.1.3 Pocket Cube Theorem

We recall from Section 3 that the configuration of the Pocket Cube $c \in C_{\mathcal{P}}$ is represented by the tuple $c = (c_\sigma, c_{\mathbf{x}})$. In Sections 4.1.1 and 4.1.2, we have successfully determined that $\forall v \in V$, $v_\sigma \in V_\sigma = i_\sigma \cdot S_8$ and $v_{\mathbf{x}} \in V_{\mathbf{x}} = i_{\mathbf{x}} \cdot (\mathbb{Z}_3)^7$. We almost have the necessary tools to prove the Pocket Cube Theorem.

Proposition 4.1.6. The group $\mathcal{P}$ contains the moves which only alters the orientation of any 2 cubies.

Proof. Let $m \in \mathcal{P}$ be the move $m = \mathbf{FU^2FU^2F^3UF^2U^3F^2UF^2}$ where $m_\sigma = e$. We use Table 1 to show the re-orientation affect of the cubies is such that $m_{\mathbf{x}} = (x_0, x_1, x_2, x_3, x_4, x_5 + 2, x_6 + 1, x_7)$ (the working is omitted). The move rotates the cubie in the ubr (5^{th}) cubicle clockwise once and the cubie in the ufr (6^{th}) cubicle clockwise twice.

In Lemma 4.1.1 we found the moves which transpose any 2 cubies which incidentally doesn't affect the orientations. Therefore we can conjugate any of these moves with m to be able to rotate any 2 cubies. □

Theorem 4.1.7. *A configuration $c = (\sigma, \mathbf{x})$ is valid if and only if $\sum x_i \equiv 0$ mod 3.*

Proof. The forward direction follows from Lemma 4.1.5 since if $c \in V$ then $\mathbf{x} \in V_{\mathbf{x}}$ and so $\sum_{i=0}^{7} x_i \equiv 0$ mod 3. The backward direction is a bit more complicated.

From any configuration $c = (\sigma, \mathbf{x})$ such that $\sum x_i \equiv 0 \bmod 3$, we can use the moves found in Proposition 4.1.6 to rotate each cubicle one by one until each of cubies are in the correct orientation. Since valid moves preserve the sum, it follows that when re-orienting the second last cubie, the final cubie will also fall into the correct orientation, giving us some sequence of moves M_1 such that $(\sigma, \mathbf{x}) \cdot M_1 = (\sigma, i_{\mathbf{x}})$.

Finally, we use the moves found in Lemma 4.1.1 to permute the cubies back into their correct positions obtaining the sequence of moves M_2 such that $(\sigma, i_{\mathbf{x}}) \cdot M_2 = (i_\sigma, i_{\mathbf{x}})$. Since $(i_\sigma, i_{\mathbf{x}})$ is the solved configuration, which, by definition, is a valid configuration, we have that $((i_\sigma, i_{\mathbf{x}}) \cdot M_2^{-1}) \cdot M_1^{-1} = (i_\sigma, i_{\mathbf{x}}) \cdot (M_2^{-1} \circ M_1^{-1}) = (\sigma, \mathbf{x})$ which is in the orbit of $i \cdot \mathcal{P}$, which are the valid configurations. □

We now have a solid theorem to understand the properties of a valid configuration and for determining whether any given configuration of the Pocket Cube is a valid one or not. What remains is to represent the group structure in a more meaningful way.

Theorem 4.1.8. $\mathcal{P} =< \boldsymbol{U,D,F,B,R,L} : R_{\mathcal{P}} > \cong S_8 \rtimes (\mathbb{Z}_3)^7$.

Proof. We have seen that each basic move can be broken down into the permutation of the cubies $\mathcal{P}_\sigma \leq \mathcal{P}$ and the re-orientation of the cubies $\mathcal{P}_{\mathbf{x}} \leq \mathcal{P}$. By Lemma 2.7.7 we have that $\mathcal{P}_\sigma \cong \mathcal{P}_\sigma \times \{e_{\mathbf{x}}\}$ and $\mathcal{P}_{\mathbf{x}} \cong \{e_\sigma\} \times \mathcal{P}_{\mathbf{x}}$. It follows that $(\mathcal{P}_\sigma \times \{e_{\mathbf{x}}\}) \cap (\{e_\sigma\} \times \mathcal{P}_{\mathbf{x}}) = \{(e_\sigma, e_{\mathbf{x}})\}$ and $\mathcal{P}_\sigma \mathcal{P}_{\mathbf{x}} = \mathcal{P}$. Finally we have that $\forall a \in \mathcal{P}$ and $\forall p \in (\{e_\sigma\} \times \mathcal{P}_{\mathbf{x}})$, $a^{-1}pa = (\sigma^{-1}, -\mathbf{x})(e_\sigma, \mathbf{x'})(\sigma, \mathbf{x}) = (\sigma^{-1}, -\mathbf{x} + \mathbf{x'})(\sigma, \mathbf{x}) = (\sigma^{-1}\sigma, -\mathbf{x} + \mathbf{x'} + \mathbf{x}) = (e_\sigma, -\mathbf{x} + \mathbf{x'} + \mathbf{x}) \in (\{e_\sigma\} \times \mathcal{P}_{\mathbf{x}})$, proving that $(\{e_\sigma\} \times \mathcal{P}_{\mathbf{x}}) \trianglelefteq \mathcal{P}$. Therefore, by Definition 2.8.4, $\mathcal{P} \cong \mathcal{P}_\sigma \rtimes \mathcal{P}_{\mathbf{x}} \cong S_8 \rtimes (\mathbb{Z}_3)^7$. □

Finally, we have the set of all valid configurations

$$V = \{(\sigma, \mathbf{x}) | \sum x_i \equiv 0 \bmod 3\}. \tag{62}$$

This effectively leaves us with a third of all the possible configurations, and so

$$|V| = 8! \times 3^7 = \mathbf{8.8179840 \times 10^7}. \tag{63}$$

4.2 Symmetries of the Pocket Cube

The Pocket Cube has multiple solved configurations. This is because there are no fixed cubies of the Pocket Cube, therefore, the spatial symmetries of the solved configuration are in its orbit. Having multiple solved configurations makes manipulating the structure of the cube tougher, which is why in Section 4.1 we ignored all solved configurations except 1. In this section we will look at understanding the relationship between the solved configurations and show that we can remove the symmetries without affecting the core group structure.

4.2.1 The Symmetry Moves Subgroup

By the rules of the Pocket Cube, there exists more than one solved configuration. There are 6 colours and we can almost arbitrarily label each of the 6 faces with a different colour to get a solved configuration, however, for it to be a valid configuration, the adjacency of the colours must be maintained. Therefore, WLOG, we start with the **Front** face and label it with one of the 6 colours, this also determines the colour of the opposite face which in this case is the **Back** face by Definition 3.1.1 of adjacency. Now we can choose any of the remaining four faces and label it with any of the remaining 4 colours, this now determines the colour of the opposite face leaving us with 2 remaining opposite faces to label with 2 remaining colours, and so we have that there are $6 \times 1 \times 4 \times 1 \times 2 \times 1 = 48$ possible solved configurations. However, this includes the mirror reflection of the cube (we will call it the mirror cube) for each configuration thus reducing the possible solved configurations to $\frac{48}{2} = 24$.

We note here that every mirrored cube configuration has a corresponding natural configuration. If the natural configuration is achieved from a natural solved configuration by the move M, its mirrored configuration is achieved by applying the move M^* to the corresponding mirrored solved configuration whereby M^* is the move M with basic moves **U, D, F, B, R, L** substituted with **U', D', F', B', L', R'** respectively, assuming the mirror is on the left (or right) of the cube.

It is impossible to go from a mirrored configuration to a natural configuration without relabelling the cube. From here we will deal only with the natural configurations, since the group of moves which act on the mirrored configurations is isomorphic to the group of moves which act on the natural configurations by the above mapping.

The remaining solved configuration, however, are all in the orbit of i under $\mathcal{P}$ and are called the spatially symmetrical solved configurations. Both the Pocket Cube and the Rubik's Cube have 24 spatial symmetries, however the main difference is that the symmetries of the Pocket Cube are reachable using the basic moves.

Definition 4.2.1. The *symmetry moves* are the set, $\mathcal{S}$, of moves which go from a solved configuration to any of the 24 solved configurations. These are the moves which rotate the entire cube by a multiple of 90° (360° gets you back the same configuration) about the x,y or z axis, as seen in Figure 10, and every unique combination of the rotations. We denote the 90° rotation about the x,y or z axis as R_x, R_y and R_z respectively where

$$R_x = RL^{-1} = L^{-1}R, \tag{64}$$

$$R_y = UD^{-1} = D^{-1}U, \tag{65}$$

$$R_z = FB^{-1} = B^{-1}F. \tag{66}$$

Proposition 4.2.2. The set of symmetry moves form a group $(\mathcal{S}, \circ)$ which is a subgroup of the Pocket Group, $S \leq \mathcal{P}$ (the Cayley graph representation of $\mathcal{S}$ is in Figure 11).

Proof. $\mathcal{S}$ is generated by the moves $\{R_x, R_y, R_z\}$ which is a subset of $\mathcal{P}$ using the same cube group operation. Therefore, by Definition 2.2.2, $\mathcal{S} \leq \mathcal{P}$. □

Corollary 4.2.3. The group of symmetry moves, $\mathcal{S}$, acts on the set of configurations, C.

Proof. This follows from Theorem 3.3.1 & 4.2.2 that since $\mathcal{P}$ is a group action on C and $\mathcal{S}$ is a subgroup of $\mathcal{P}$, $\mathcal{S}$ is a group action on C. □

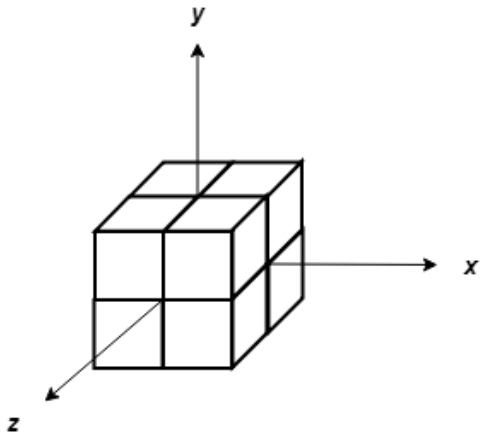

Figure 10: Axes of the Pocket Cube.

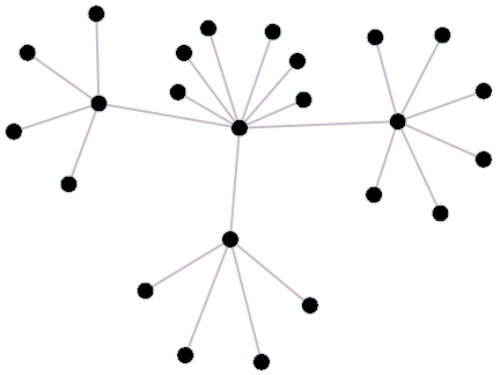

Figure 11: Cayley graph representation of the symmetry moves group $\mathcal{S}$.

4.2.2 Simplifying the Pocket Group

Definition 4.2.4. The *state* of the Pocket Cube is the position and orientation of each cubie relative to one another, irrespective of the cubicles they are in. That is, the 24 different spatial symmetries of a configuration, all having different configurations, are said to be in the same state.

We've seen that there are 24 different spatial symmetries, or configurations, of the solved state. These symmetries, however, are not limited to just the solved state. Each and every state of the Pocket Cube has 24 symmetries and therefore 24 different representations in terms of its configuration. Intuitively, the symmetry moves don't actually slide any cubies over one another, therefore, we say that they preserve the position and orientation of the cubies in relation to one another and so these moves do not alter the state of the Pocket Cube. In other words the 24 different configurations of a state are equivalent. We do this more formally by Proposition 4.2.5.

Proposition 4.2.5. The binary relation $\sim$ on the set of configurations, C, is an equivalence relation $x \sim y \iff \exists s \in \mathcal{S}$ such that $(x, s)\phi = x \cdot s = y$.

Proof. We have that $\forall x \in C, x \sim x$ since $e \in \mathcal{S}$ and $x \cdot e = x$. Suppose $x \sim y$ s.t. $x \cdot s = y$ for some $s \in \mathcal{S}$ and $y \in C$, then $y \cdot s^{-1} = (x \cdot s) \cdot s^{-1} = x \cdot (s \circ s^{-1}) = x$ and so $y \sim x$. Finally, if $x \sim y$ and $y \sim z$ s.t. $x \cdot s = y$ and $y \cdot t = z$ for some $s, t \in \mathcal{S}$ then $x \cdot (s \circ t) = (x \cdot s) \cdot t = y \cdot t = z$ and so $x \sim z$. □

Remark 4.2.6. Let $x \cdot \mathcal{S}$ denote the equivalence class of the configuration $x \in C$ such that $x \cdot \mathcal{S} = \{y \in C | x \sim y\} = \{y \in C | \exists s \in \mathcal{S}, x \cdot s = y\} = \{x \cdot s | \forall s \in \mathcal{S}\}$.

This means that the equivalence class for a solved configuration is the set of all configurations in a solved state, which are the solved configurations. We now see that each state of the cube is represented by an equivalence class and so a symmetry move takes a configuration to one within its equivalence class.

$$x \cdot R_x \equiv x \cdot R_y \equiv x \cdot R_z \equiv x \cdot e \tag{67}$$

and more generally $\forall m \in \mathcal{S} \leq \mathcal{P}$ and $\forall x \in C, x \cdot m \equiv x \cdot e$ where e is the identity move of the Pocket Group $\mathcal{P}$, the do nothing move.

Each equivalence class $x \cdot \mathcal{S}$ is an orbit which has 24 elements and therefore partitions the set C into $|C|/24$ orbits. We note here that we could have achieved the same partitioning with the set of left cosets $\mathcal{P}/\mathcal{S}$. When applying this to the set of valid configurations V, we partition V into $|V|/24 = 3,674,160$ orbits. We define a set $W \subseteq V$ to be the **representative set** (Definition 4.2.7) for the orbits of V under $\mathcal{S}$ (i.e. $v \cdot \mathcal{S}$, $\forall v \in V$).

Definition 4.2.7. Let G be a group which acts on a set X such that $X = x \cdot G, x \in X$. Let H be a subgroup of G. The *representative set* for the orbits of H under X is the coset representative [12] of the set of left cosets G/H. It is the set which contains 1 element from each orbit (or left coset).

Proposition 4.2.8. The Pocket Group whose orbit forms the representative set W, denoted as $\mathcal{Q}$, can be generated by 3 basic moves. In particular, $\mathcal{Q} =<$ **U, F, R** $>$.

Proof. The Pocket Group is generated by the 6 basic moves; **U, D, F, B, R** and **L**. We have that the equivalence relation in equation 67 holds and so we can simplify the action of the following moves using equations 64, 65 and 66; $\forall v \in V$

$$v \cdot D \equiv (v \cdot D) \cdot R_y = v \cdot (D(D^{-1}U)) = v \cdot (DD^{-1})U = v \cdot U, \tag{68}$$

$$v \cdot B \equiv (v \cdot B) \cdot R_z = v \cdot (B(B^{-1}F)) = v \cdot (BB^{-1})F = v \cdot F, \tag{69}$$

$$v \cdot L \equiv (v \cdot L) \cdot R_x = v \cdot (L(L^{-1}R)) = v \cdot (LL^{-1})R = v \cdot R. \tag{70}$$

The group action of the basic moves **D, B** and **L** on the set of configurations is respectively equivalent to the group action of **U, F** and **R**. This means that WLOG **U** and **D** take a configuration into the same equivalence class, which gives us redundancies, and so we can reduce the number of generators of the group to the 3 basic moves **U, F** and **R** which effectively removes any extra configurations from the same equivalence class. Therefore, the orbits of the simplified Pocket Group $\mathcal{Q} =<$ **U, F, R** $>$ only have one configuration from each equivalence class $v \cdot \mathcal{S}$ (implying only one solved configuration), and so forms the representative set W for the orbits of V under $\mathcal{S}$. □

Remark 4.2.9. The orbits of $x \cdot Q$ are the possible representative sets of $x \cdot \mathcal{S}$. WLOG $x \in C$ or $x \in V$.

Corollary 4.2.10. $\forall v \in V, |v \cdot Q| = 3,674,160$.

Proof. This follows from Remark 4.2.9 and the fact that there are 3,674,160 orbits of V under the symmetry group $\mathcal{S}$. □

Intuitively, this fixes one of the cubies in a cubicle by removing the moves that permute the cubie in that cubicle. In particular, for $\mathcal{Q} =<$ **U, F, R** $>$ the cubie in the the down, back and left cubicle (dbl using Janet's notation [7]) is fixed, as seen in Figure 12.

There are two things to note here:

1) There are 8 possible ways to choose the generators for the simplified Pocket Group, each of which fixes the cubie of a different cubicle and is isomorphic to each other.

2) There are 8 different cubies we can choose to be fixed in WLOG the dbl cubicle, and for each choice we can fix the cubie in 3 possible orientations giving us $8 \times 3 = 24$ orbits of the simplified Pocket Group.

Again, we face the issue that defining the simplified Pocket Group using its generators and generator relations doesn't tell us much about the structure of the group. Hence, we define the group as we did in

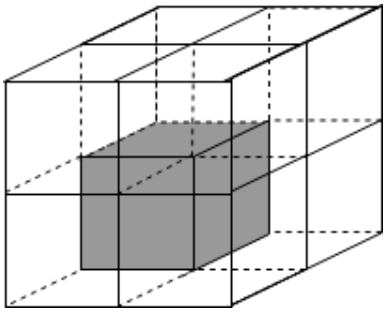

Figure 12: Visualisation of the fixed cubie in the dbl cubicle.

Section 4.1.3; since $\mathcal{Q}$ only removes spatial symmetries, we have that the moves can still freely permute the remaining 7 cubies and can re-orient them to maintain $\sum_{i=1}^{7} x_i$ where the cubicle indexed 0 is fixed. Therefore, we have that the simplified Pocket Group is

$$\mathcal{Q} =< \mathbf{U},\ \mathbf{F},\ \mathbf{R} > \tag{71}$$

$$= S_7 \times (\mathbb{Z}_3)^6. \tag{72}$$

Finally, we have that the simplified Pocket Group $\mathcal{Q}$ acts on the set of valid configurations V. The orbit of a solved configuration, WLOG $(i_\sigma, i_{\mathbf{x}})$, under $\mathcal{Q}$ is the set of valid configurations with the initial cubie in the dbl cubicle fixed and with only one solved configuration; since there are no spatially symmetrical configurations in the same orbit. Therefore, since there are 24 different starting solved configurations, there are 24 different orbits of the action $\mathcal{Q}$ on V and so

$$|V_{\mathcal{Q}}| = |v \cdot \mathcal{Q}| = 3,674,160. \tag{73}$$

4.3 The Rubik's Cube

4.3.1 Permutations of the Cubies

In order to consider only the permutations, we have to ignore the orientation of the cubies and have that a move is some permutation of the cubies, in this case, the 8 corner cubies and 12 edge cubies.

Since, we only care about the permutations of the cubies - the position in terms of which cubicle a cubie is in and which cubicle it is moved to after applying a move - we label the cubicles using Janet's notation [7] and, equivalently, index them using the numbers 0 to 7 for the corner cubies, as seen in Figure 8 and 0 to 11 for the edge cubies, as seen in Figure 13 where the 0th (dl), 3rd (db) and the 7th (lb) cubicles are hidden [2].

We can now define each of the 6 basic moves as the following permutations of the corner cubies;

$$\mathbf{U}_\sigma = (\text{ubl, ubr, ufr, ufl}) = (4,\ 5,\ 6,\ 7), \tag{74}$$

$$\mathbf{D}_\sigma = (\text{dbl, dfl, dfr, dbr}) = (0,\ 1,\ 2,\ 3), \tag{75}$$

$$\mathbf{F}_\sigma = (\text{dfl, ufl, ufr, dfr}) = (1,\ 7,\ 6,\ 2), \tag{76}$$

$$\mathbf{B}_\sigma = (\text{dbl, dbr, ubr, ubl}) = (0,\ 3,\ 5,\ 4), \tag{77}$$

$$\mathbf{R}_\sigma = (\text{ufr, ubr, dbr, dfr}) = (2,\ 6,\ 5,\ 3), \tag{78}$$

$$\mathbf{L}_\sigma = (\text{dbl, ubl, ufl, dfl}) = (0,\ 4,\ 7,\ 1); \tag{79}$$

[2] We label the cubies by counting them in the manner of anti-clockwise from the bottom.

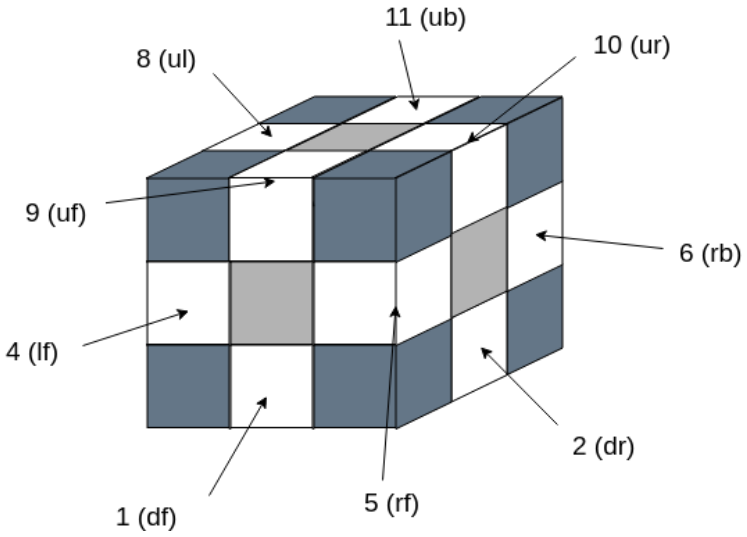

Figure 13: Indexing of the edge cubicles.

and the following permutations of the edge cubies;

$$\mathbf{U}_\tau = (\text{ul, ub, ur, uf}) = (8, 11, 10, 9), \tag{80}$$
$$\mathbf{D}_\tau = (\text{dl, df, dr, db}) = (0, 1, 2, 3), \tag{81}$$
$$\mathbf{F}_\tau = (\text{df, lf, uf, rf}) = (1, 4, 9, 5), \tag{82}$$
$$\mathbf{B}_\tau = (\text{db, rb, ub, lb}) = (3, 6, 11, 7), \tag{83}$$
$$\mathbf{R}_\tau = (\text{dr, rf, ur, rb}) = (2, 3, 10, 6), \tag{84}$$
$$\mathbf{L}_\tau = (\text{dl, lb, ul, lf}) = (0, 7, 8, 4). \tag{85}$$

This means that the permutation of the cubies by a valid move m is the permutation of the 8 corner cubies, $m_\sigma \in S_8$, and the 12 edge cubies, $m_\tau \in S_{12}$. The corner cubie permutations form the subgroup $\mathcal{R}_\sigma =< \mathbf{U}_\sigma, \mathbf{D}_\sigma, \mathbf{F}_\sigma, \mathbf{B}_\sigma, \mathbf{R}_\sigma, \mathbf{L}_\sigma >$ of S_8 and the edge cubie permutations form the subgroup $\mathcal{R}_\tau =< \mathbf{U}_\tau, \mathbf{D}_\tau, \mathbf{F}_\tau, \mathbf{B}_\tau, \mathbf{R}_\tau, \mathbf{L}_\tau >$ of S_{12}. We note that by comparing $\mathcal{R}_\sigma$ to $\mathcal{P}_\sigma$ we can clearly see that $\mathcal{R}_\sigma = \mathcal{P}_\sigma$.

If we continue to assume that the corner cubies and the edge cubies can be freely permuted then the permutation of the cubies can be represented by the group $S_8 \times S_{12}$, however, this is not the case.

Each basic move $b \in \mathcal{B}$ has a corresponding b_σ and b_τ; both of which are 4-cycles and have an odd parity (Definition 2.5.5), denoted by $sgn(b_\sigma) = sgn(b_\tau) = -1$ (following Janet's notation [7]). When applying a basic move, we need to apply both the permutation of the corner cubies and the edge cubies and so we can compose them together to get the overall permutations of the move b such that $b_{\sigma\tau} = b_\sigma \circ b_\tau$ where order doesn't matter, however, as convention we will permute the corners followed by the edges.

We can now define the overall permutation of the cubies by the 6 basic moves as the following[3];

$$\mathbf{U}_{\sigma\tau} = (\text{ubl, ubr, ufr, ufl})(\text{ul, ub, ur, uf}), \tag{86}$$
$$\mathbf{D}_{\sigma\tau} = (\text{dbl, dfl, dfr, dbr})(\text{dl, df, dr, db}), \tag{87}$$
$$\mathbf{F}_{\sigma\tau} = (\text{dfl, ufl, ufr, dfr})(\text{df, lf, uf, rf}), \tag{88}$$
$$\mathbf{B}_{\sigma\tau} = (\text{dbl, dbr, ubr, ubl})(\text{db, rb, ub, lb}), \tag{89}$$
$$\mathbf{R}_{\sigma\tau} = (\text{ufr, ubr, dbr, dfr})(\text{dr, rf, ur, rb}), \tag{90}$$
$$\mathbf{L}_{\sigma\tau} = (\text{dbl, ubl, ufl, dfl})(\text{dl, lb, ul, lf}). \tag{91}$$

[3]To avoid confusion, we will use Janet's notation.

Since the composition of 2 odd permutations is even we have that the basic moves $b_{\sigma\tau}, \forall b \in \mathcal{B}$, are even permutations.

Lemma 4.3.1. If $m \in \mathcal{R}$ is valid then the corresponding corner and edge cubie permutations of the move, m_σ and m_τ are such that $sgn(m_\sigma) = sgn(m_\tau)$.

Proof. Let $m \in \mathcal{R}$ where $m = b_1 b_2 ... b_n$. It follows that $\exists m_\sigma, m_\tau$ such that $m_\sigma = b_{1_\sigma} b_{2_\sigma} ... b_{n_\sigma}$ and $m_\tau = b_{1_\tau} b_{2_\tau} ... b_{n_\tau}$. We have that $\forall b \in \mathcal{B}$, the permutations of corner and edge cubies are respectively 4-cycles and so $sgn(b_\sigma) = sgn(b_\tau) = -1$. We easily see that $sgn(m_\sigma) = (-1)^n$ and similarly $sgn(m_\tau) = (-1)^n$. Therefore $sgn(m_\sigma) = sgn(m_\tau) = (-1)^n$. □

Corollary 4.3.2. If $m \in \mathcal{R}$ is valid then the permutation of the cubies $m_{\sigma\tau}$ is an even permutation.

Proof. Let $m \in \mathcal{R}$ be a valid move. By Lemma 4.3.1, $sgn(m_\sigma) = sgn(m_\tau)$ and so $sgn(m_{\sigma\tau}) = sgn(m_\sigma \circ m_\tau) = sgn(m_\sigma) sgn(m_\tau) = (sgn(m_\sigma))^2 = (\pm 1)^2 = 1$. □

This means that only half of all the possible permutations of $S_8 \times S_{12}$ are valid permutations of the Rubik's Cube; and these are only the permutations $m_{\sigma\tau} \in \mathcal{R}_{\sigma\tau} = \{(m_\sigma, m_\tau) \in S_8 \times S_{12} : sgn(m_\sigma) = sgn(m_\tau)\}$. We have disproved our initial assumption that we can freely permute the cubies.

Lemma 4.3.3. $\mathcal{R}_{\sigma\tau} \cong ((A_8 \times A_{12}) \ltimes \mathbb{Z}_2)$.

Proof. We define a homomorphism $\phi : \mathcal{R}_{\sigma\tau} \to \mathbb{Z}_2$ such that $\forall m_{\sigma\tau} \in \mathcal{R}_{\sigma\tau}$, $m_{\sigma\tau} \mapsto sgn(m_\sigma)$. It follows by Lemma 4.3.1 and since $sgn(m_\sigma) = 0$ (refer to Example 2.7.8) when m_σ is an even permutation that $ker(\phi) = (A_8 \times A_{12})$. By Lemma 2.7.6 $ker(\phi)$ is a normal subgroup of $R_{\sigma\tau}$. We have that $\mathbb{Z}_2 \cong H =< (dbl, ubl)(db, lb) >= \{e_\sigma e_\tau, (dbl, ubl)(db, lb)\}$. Since $H \cap ker(\phi) = \{e_\sigma e_\tau\}$ and $H ker(\phi) = \mathcal{R}_{\sigma\tau}$, we have that $\mathcal{R}_{\sigma\tau} \cong ker(\phi) \ltimes < (dbl, ubl)(db, lb) > \cong ((A_8 \times A_{12}) \ltimes \mathbb{Z}_2)$. □

Intuitively this makes sense. If we had just the alternating group $(A_8 \times A_{12})$ we would only have the permutations where the corner and edge permutations were even. In order to get the ones where they are both odd, we need to apply a transposition to both the corner and edge permutations.

Thus the valid permutations of the Rubik's cube $V_{\sigma\tau}$ is the orbit of (i_σ, i_τ) under $\mathcal{R}_{\sigma\tau}$ such that $V_{\sigma\tau} = (i_\sigma, i_\tau) \cdot ((A_8 \times A_{12}) \ltimes \mathbb{Z}_2)$.

4.3.2 Orientations of the Cubies

Firstly, we need to define some notation for the orientation of the cubies. We start by looking at the cube in the solved configuration, in this configuration we know that each cubie is correctly positioned and, more importantly, correctly oriented. For the case of the Rubik's Cube we have two types of cubies, the corner and edge ones. We will deal with their orientations separately.

Corner Cubies

The orientation of the corner cubies of the Rubik's cube are analogous to that of the Pocket Cube (see Section 4.1.2). Therefore we have that $\mathcal{R}_{\mathbf{x}} = \mathcal{P}_{\mathbf{x}} = (\mathbb{Z}_3)^7$.

Edge Cubies

It remains that there are 12 edge cubies, each of which can be oriented in 2 different ways, the correct one being its orientation in the solved configuration. The edge cubies have only 2 orientations and so are either in a correct orientation or not, therefore, we can model this behaviour using the additive group of integers modulo 2, $\mathbb{Z}_2$.

The orientation of each cubie in any given state can be denoted using $y_i \in \mathbb{Z}_2, \forall i = 0, 1, ..., 11$. We begin by labelling the facet of each cubie which is in either the **Up** or **Down** face (it's easy to see that a single cubie can't have facets in both) with y_i where i is the index of the cubie as defined in Figure 13. For the remaining 4 cubies we label the facets on the **Front** and **Back** faces with y_i. Next we label the other facet of each cubie with $y_i + 1$ as depicted in Figure 14.

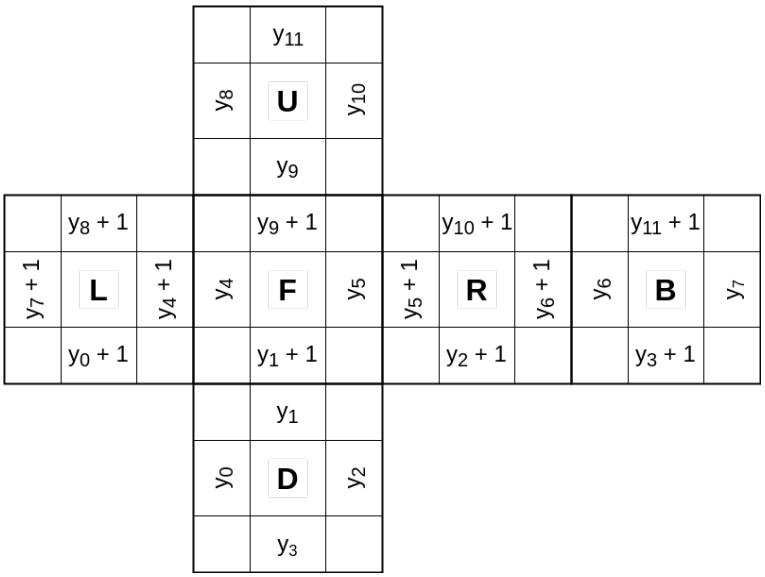

Figure 14: Labelled orientation of the edge cubies

Definition 4.3.4. The orientation of the edge cubies is represented by the tuple $\mathbf{y} = (y_0, y_1, ..., y_{11}), y_i \in \mathbb{Z}_2$ and in a solved configuration $y_i = 0$, $\forall i = 0, 1, ..., 11$.

We now have a way to represent the orientations of each edge cubie. By starting from an arbitrary orientation of the cube, $\mathbf{y} = (y_0, y_1, ..., y_{11})$, we get the orientations of the cube in Table 2 after applying each of the basic moves.

Move	**Orientation, $\vec{y'}$, after applying a move**
$\mathbf{U_y}$	$(y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_9, y_{10}, y_{11}, y_8)$
$\mathbf{D_y}$	$(y_3, y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11})$
$\mathbf{F_y}$	$(y_0, y_5 + 1, y_2, y_3, y_1 + 1, y_9 + 1, y_6, y_7, y_8, y_4 + 1, y_{10}, y_{11})$
$\mathbf{B_y}$	$(y_0, y_1, y_2, y_7 + 1, y_4, y_5, y_3 + 1, y_{11} + 1, y_8, y_9, y_{10}, y_6 + 1)$
$\mathbf{R_y}$	$(y_0, y_1, y_6, y_3, y_4, y_2, y_{10}, y_7, y_8, y_9, y_5, y_{11})$
$\mathbf{L_y}$	$(y_4, y_1, y_2, y_3, y_8, y_5, y_6, y_0, y_7, y_9, y_{10}, y_{11})$

Table 2: Re-orientations of the edge cubies by the basic moves

If we continue to assume that we can freely re-orient the cubies, then the change in orientation of the cubies can be represented by the group $(\mathbb{Z}_2)^{12}$, however, this is not the case.

Proposition 4.3.5. If $m \in \mathcal{P}$, a valid move, then $\sum y_i \equiv \sum y'_i \mod 2$ where $\vec{y'}$ is the orientation of the edge cubies after applying the move m.

Proof. We take the orientation of the cubies to be the tuple $\mathbf{y} \in (\mathbb{Z}_2)^{12}$ where $\sum y_i \equiv a \mod 2$ $\forall i = 0, ..., 11$. Upon applying each of the moves, we get the orientations in Table 2.

It follows that for the case after move **U**, **D**, **R** or **L**, $\sum y'_i = \sum y_i \equiv a \mod 2$, and, also, for the case after moves **F** or **B**, $\sum y'_i = \sum y_i + 4 \equiv a \mod 2$. □

We now have that the re-orientations of the cubies preserve the $\sum_{i=0}^{11} y_i$ which is equivalent to freely choosing the orientation of 11 cubies, since the last one is set to preserve $\sum_{i=0}^{11} y_i$. Therefore, the group which represents the valid re-orientation of the edge cubies is $\mathcal{R}_\mathbf{y} = (\mathbb{Z}_2)^{11}$.

Corner and Edge Cubies

There are no additional constraints on the re-orientaton of the cubies by a valid move and so we can combine the two groups using the direct product such that $\mathcal{R}_{\mathbf{xy}} = \mathcal{R}_{\mathbf{x}} \times \mathcal{R}_{\mathbf{y}} = (\mathbb{Z}_3)^7 \times (\mathbb{Z}_2)^{11}$.

We have that the orientations of the Rubik's Cube in a solved configuration is $(i_{\mathbf{x}}, i_{\mathbf{y}})$ where $i_{\mathbf{x}} = \mathbf{0} = (0,0,0,0,0,0,0,0)$ and $i_{\mathbf{y}} = \mathbf{0} = (0,0,0,0,0,0,0,0,0,0,0,0)$. The set of valid orientations $V_{\mathbf{xy}}$ of the Rubik's cube is the orbit of the solved configuration $(i_{\mathbf{x}}, i_{\mathbf{y}})$ under $\mathcal{R}_{\mathbf{xy}}$ such that $V_{\mathbf{xy}} = (i_{\mathbf{x}}, i_{\mathbf{y}}) \cdot ((\mathbb{Z}_3)^7 \times (\mathbb{Z}_2)^{11})$.

Lemma 4.3.6. If $(\mathbf{x}, \mathbf{y}) \in V_{\mathbf{xy}}$ then $\sum_{i=0}^{7} x_i \equiv 0 \bmod 3$ and $\sum_{i=0}^{11} y_i \equiv 0 \bmod 2$.

Proof. It follows from Section 3.3, Proposition 4.1.4 and Proposition 4.3.5 that $V_{\mathbf{xy}} = (\mathbf{v}, \mathbf{w}) \cdot \mathcal{R}_{\mathbf{xy}}$ where $\mathbf{v} = \mathbf{0}$ and $\mathbf{w} = \mathbf{0}$, and since every valid move preserves the respective sums, we have that $\forall (\mathbf{x}, \mathbf{y}) \in V_{\mathbf{xy}}, \sum_{i=0}^{7} x_i \equiv \sum_{i=0}^{7} v_i \equiv 0 \bmod 3$ and $\sum_{i=0}^{11} y_i \equiv \sum_{i=0}^{11} w_i \equiv 0 \bmod 2$. □

4.3.3 Rubik's Cube Theorem

We recall from Section 3 that the configuration of the Rubik's Cube $c \in C_{\mathcal{R}}$ is represented by the tuple $c = (c_\sigma, c_\tau, c_{\mathbf{x}}, c_{\mathbf{y}})$. In Sections 4.3.1 and 4.3.2, we have successfully determined that $\forall v \in V$, $(v_\sigma, v_\tau) \in V_{\sigma\tau} = (i_\sigma, i_\tau) \cdot ((A_8 \times A_{12}) \ltimes \mathbb{Z}_2)$ and $(v_{\mathbf{x}}, v_{\mathbf{y}}) \in V_{\mathbf{xy}} = (i_{\mathbf{x}}, i_{\mathbf{y}}) \cdot ((\mathbb{Z}_3)^7 \times (\mathbb{Z}_2)^{11})$. We almost have the necessary tools to prove the Rubik's Cube Theorems.

Proposition 4.3.7. The Rubiks Group $\mathcal{R}$ contains the move that cycles 3 edge cubies without affecting the corner cubies.

Proof. We find the move $m0 = \mathbf{LR^{-1}U^2L^{-1}RB^2} = (ub, uf, db)$ [7]. It is easy to show that for any edge cubie C_1, C_2 and C_3 there exists a move $m \in \mathcal{R}$ which takes the cubie in the ub cubicle to C_1, the cubie in the uf cubicle to C_2 and the cubie in the db cubicle to C_3. Therefore, we have that the conjugate $m^{-1}m_0m = (C_1, C_2, C_3)$. □

Proposition 4.3.8. The Rubik's Group $\mathcal{R}$ contains the moves that only re-orients any 2 cubies without affecting any positions or the orientations of any other cubies.

Proof. We find the move

$$m = \mathbf{LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}B^{-1}LR^{-1}U^{-1}}. \tag{92}$$

We use Table 2 to show the re-orientation affect of the cubies is such that

$$m_{\mathbf{y}} = (y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9 + 1, y_{10}, y_{11} + 1) \tag{93}$$

(the working is omitted). The move flips the cubies in the uf (9^{th}) and ub (11^{th}) cubicles. We saw in Proposition 4.3.7 that we can send ub to C_1 and uf to C_2, therefore, we have that we can flip the orientation of any C_1 and C_2 without affecting the positions and orientations of any other cubies. □

Theorem 4.3.9. *A configuration $c = (\sigma, \tau, \mathbf{x}, \mathbf{y})$ is valid if and only if $sgn(\sigma) = sgn(\tau)$, $\sum x_i \equiv 0$ mod 3 and $\sum y_i \equiv 0$ mod 2.*

Proof. The forward direction follows from Lemmas 4.3.1 and 4.3.6. If $v \in V$ then there exists some $m \in \mathcal{R}$ such that $i \cdot m = v$ and so $sgn(m_\sigma) = sgn(m_\tau)$. Also, if $v \in V$ then $(v_{\mathbf{x}}, v_{\mathbf{y}}) \in V_{\mathbf{xy}}$ and so $\sum x_i \equiv 0 \bmod 3$ and $\sum y_i \equiv 0 \bmod 2$. The backward direction is a bit more tricky.

From any configuration $c = (\sigma, \tau, \mathbf{x}, \mathbf{y})$ such that $sgn(\sigma) = sgn(\tau)$, $\sum x_i \equiv 0 \bmod 3$ and $\sum y_i \equiv 0 \bmod 2$, we use the steps in the proof of the backward direction of Theorem 4.1.3 to get $(\sigma, \tau, \mathbf{x}, \mathbf{y}) \cdot (M_1 \circ M_2) = (i_\sigma, \tau', i_{\mathbf{x}}, \mathbf{y}')$. All moves m used from here need to preserve the corner cubies, in particular, we have that $m_\sigma = e_\sigma \implies sgn(m_\sigma) = 0 \implies sgn(m_\tau) = 0$ and so only even permutations of the edge cubies are allowed.

In Proposition 4.3.7 we found the moves which cycles any 3 edge cubies without affecting the corner cubies. We apply these moves such that whenever a cubie is in the correct cubicle, we swap to another 3 cycle until it remains that 3 edge cubies are incorrectly positioned and so the final 3 cycle will put

them in the correct positions. We obtain a sequence of these moves M_3 such that $(i_\sigma, \tau', i_\mathbf{x}, \mathbf{y}') \cdot M_3 = (i_\sigma, i_\tau, i_\mathbf{x}, \mathbf{y}'')$.

Finally, we use the moves found in Proposition 4.3.8 to re-orient the flipped cubies by the sequence of moves, and since the valid moves preserves the sums, we have that $\sum y_i'' \equiv 0 \bmod 2$, we will eventually get to the edge cubies correctly oriented by the sequence of moves M_4 such that $(i_\sigma, i_\tau, i_\mathbf{x}, \mathbf{y}'') \cdot M_4 = (i_\sigma, i_\tau, i_\mathbf{x}, i_\mathbf{y})$ which is the solved configuration. We now have that $(i_\sigma, i_\tau, i_\mathbf{x}, i_\mathbf{y}) \cdot (M_4^{-1} \circ M_3^{-1} \circ M_2^{-1} \circ M_1^{-1}) = (\sigma, \tau, \mathbf{x}, \mathbf{y})$ is in the orbit $i \cdot \mathcal{R}$, which is the set of valid configurations. □

We now have a solid theorem to understand the properties of a valid configuration and for determining whether any given configuration of the Rubik's Cube is a valid one or not. What remains is to represent the group structure in a more meaningful way.

Theorem 4.3.10. $\mathcal{R} =< \boldsymbol{U,D,F,B,R,L} : R_\mathcal{R} > \cong ((A_8 \times A_{12}) \ltimes \mathbb{Z}_2) \rtimes ((\mathbb{Z}_3)^7 \times (\mathbb{Z}_2)^{11})$.

Proof. Analogous to the proof from Theorem 4.1.8 where we consider the subgroup $\mathcal{R}_{\sigma\tau}$ and normal subgroup $\mathcal{R}_\mathbf{xy}$ giving us $\mathcal{R} \cong \mathcal{R}_{\sigma\tau} \rtimes \mathcal{R}_\mathbf{xy} \cong ((A_8 \times A_{12}) \ltimes \mathbb{Z}_2) \rtimes ((\mathbb{Z}_3)^7 \times (\mathbb{Z}_2)^{11})$. □

Finally, we have the set of all valid configurations

$$V = \{(\sigma, \tau, \mathbf{x}, \mathbf{y}) | sgn(\sigma) = sgn(\tau), \sum x_i \equiv 0 \bmod 3 \text{ and } \sum x_i \equiv 0 \bmod 3\}. \tag{94}$$

This effectively leaves us with a twelfth of all the possible configurations, and so

$$|V| = \frac{8! \times 3^7 \times 12! \times 2^{11}}{2} = \mathbf{4.3252003 \times 10^{19}}. \tag{95}$$

4.4 Conclusion

Overall, we saw that describing the group using its generators was very useful for understanding the generic structure of the Pocket and Rubik's Cube. Both groups could be represented by $\mathcal{G} =< \mathbf{U,D,F,B,R,L} >$ where their differences were encapsulated in the generator relations $R_\mathcal{P}$ and $R_\mathcal{R}$. However, these were too complicated to intuitively understand the groups.

The approach using direct and semi-direct products, on the other hand, whereby $\mathcal{P} \cong S_8 \rtimes (\mathbb{Z}_3)^7$ and $\mathcal{R} \cong ((A_8 \times A_{12}) \ltimes \mathbb{Z}_2) \rtimes ((\mathbb{Z}_3)^7 \times (\mathbb{Z}_2)^{11})$ was much more informative. From here we can already determine the structure of a valid move. In the case of a Pocket Cube move it can freely permute the cubies, however, the sum of the orientatons is preserved. We can similarly see that a Rubik's Cube move only has half the possible cube permutations and a sixth of the possible orientations.

We note here, however, that both methods of presenting the groups have their benefits and we will see in the next part that the group $\mathcal{P}$ defined using its generators is used to find God's Number.

We, also, saw that the Pocket Cube Group, which has no fixed cubies, could be simplified to the group $\mathcal{Q} =< \mathbf{U,F,R} >$ by fixing a cubie of the Pocket Cube, and removing the basic moves which changes it's orientation or position. This method can be generalised for any cube without a fixed point, so for any $n \times n \times n$ Rubik's cube where n is even.

Finally, we saw that the corner cubies for the Rubik's Cube and for the Pocket Cube were affected the same way by the basic moves. This means that if we ignored the edge and center cubies of the Rubik's cube, it would behave like the Pocket Cube. Intuitively, it is the same as relabelling the Rubik's Cube as in Figure 15.

Formally, it is the homomorphism

$$\phi : \mathcal{R} \to \mathcal{P} \tag{96}$$

$$(\sigma, \tau, \mathbf{x}, \mathbf{y}) \mapsto (\sigma, i_\tau, \mathbf{x}, i_\mathbf{y}). \tag{97}$$

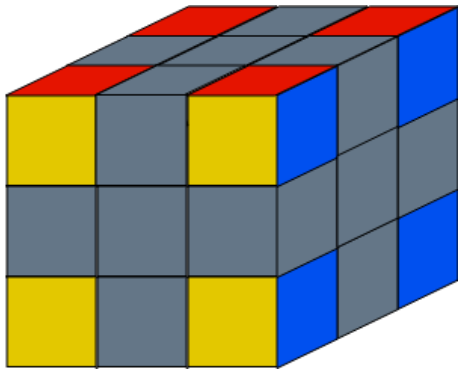

Figure 15: Relabelling of the Rubik's Cube

Part II
God's Number

We have now mathematically described the Pocket and Rubik's Cube using two different methods. The direct and semi-direct products helped us understand the configurations of the cubes, however, in this part, we will be using the generators to tackle the problem of finding God's Number for the Pocket Cube.

5 Defining God's Number

Definition 5.0.1. Let $(G, \circ)$ be a group with generating set S, $(G, \circ) =< S >$. Then the Cayley graph, $\mathcal{C}_G$, is a graph with vertex set $V(\mathcal{C}_G) = G$ and edge set $E(\mathcal{C}_G) = \{(g, g \circ s) : g \in G, s \in S\}$ where loops in the Cayley Graph correspond to generator relations [9].

Every group G with generating set S can be represented using a **Cayley Graph** (Definition 5.0.1). In terms of the Pocket Group $\mathcal{P}$ (or the Rubik's group), the elements of $\mathcal{P}$ make up the vertex set of the Cayley Graph. The generators of $\mathcal{P}$ are the set of basic moves B, each of which represent a different type of edge. For every move $m \in \mathcal{P}$ and $b \in B$, the vertices m and $b \circ m$ are connected by a b-type edge.

We can use the left group action to create the orbit of $\mathcal{P}$ under a solved configuration, WLOG $a = (i_\sigma, i_{\mathbf{x}}) \in V$, which effectively changes the vertex set from the elements of $\mathcal{P}$ to their corresponding elements in $a{\cdot}\mathcal{P}$. This means that if we wanted to find the sequence of moves between any 2 configurations, all we need to do is find a path between their respective vertices. In order to find God's number, we need to find the shortest path from every valid configuration to a solved configuration, this is effectively the depth of the Cayley Graph of $\mathcal{P}$ from the identity move. Formally, it is the eccentricity of $e \in \mathcal{P}$ of the Cayley Graph of $\mathcal{P}$ [17].

We note here that the elements of $\mathcal{P}$ are all canonical sequences of shortest length due to the generator relations of the group. Otherwise $\mathcal{P}$ would be an infinite group. We may allow cycles where the cycles formed are the generator relations (not necessarily the independent ones). If that was the case there would be multiple unique paths between vertices and so the Cayley Graph of $\mathcal{P}$ would contain cycles [17].

For example, $\mathbf{U}^4\mathbf{F} \notin \mathcal{P}$ because $\mathbf{U}^4\mathbf{F} = \mathbf{eF} = \mathbf{F} \in \mathcal{P}$.

Example 5.0.2. Let the group G = $\mathbb{Z}_8^+$ = {0,1,2,3,4,5,6,7}. We associate this to the cube group by using +1 to represent the basic moves which generates the other moves, -1 as its inverse, and the element 0 representing the solved configuration. In group G, element 4 is the furthest element from 0 at a distance of 4 (this is either +1+1+1+1=+4 or -1-1-1-1=-4 but WLOG we only keep one of the shortest path) and so the *eccentricity*(0) of the cayley graph is 4 which represents God's Number. Figure 16 is the Cayley Graph that describes this orbit of the element 0 uder G. If we included both sequence +1+1+1+1 and -1-1-1-1 (creating a cycle) we would also have to include the sequence +1+1+1+1+1+1-1-1 and the

infinite number of possible sequences (including all cycles) to attain 4 from 0, which would increase the *eccentricity*(0) of the graph to an undefined length or ∞.

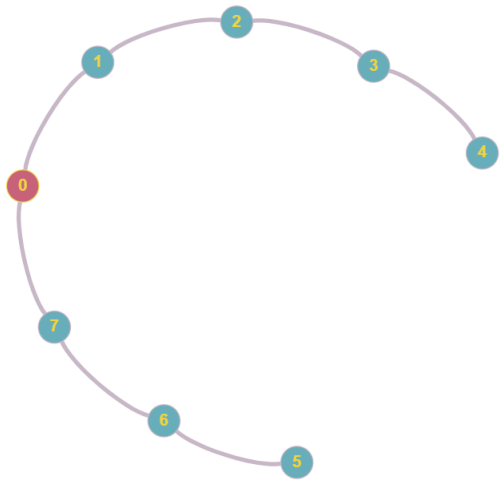

Figure 16: Cayley Graph of $\mathbb{Z}_8^+$

Example 5.0.3. Let the group $G = \mathbb{Z}_3 \times \mathbb{Z}_3$. We can define similar notions of the group as in example 5.0.2, however in this case we have 2 generators for the group and therefore 2 types of edges. We have that $G =< (0,1), (1,0) >$ each of which correspond to the action of the 2 types of edges in the Cayley Graph as seen in Figure 17. We can easily show, or see from the graph, that the *eccentricity*(0) of the graph is 2.

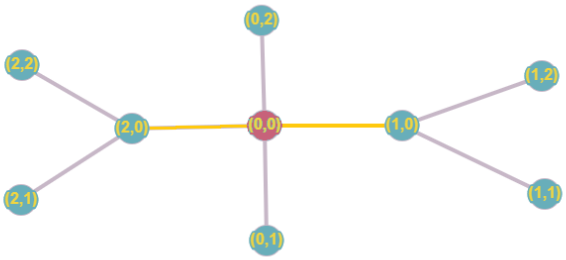

Figure 17: Cayley Graph of $\mathbb{Z}_3 \times \mathbb{Z}_3$

6 Finding God's Number

Finding God's number for the Pocket Cube can be computed using the brute force method to show that it is in fact 11 with the half-turn metric and 14 with the quarter-turn metric, however, it we will see later that group $\mathcal{P}$ is too large.

In this section, we will look at the brute force method and the initial method by Thistlethwaite, which greatly influenced the subsequent methods.

6.1 Thistlethwaite's Algorithm

In this section we will look at the algorithm in terms of the Rubik's Cube, and in the later section, we will apply it on the Pocket Cube.

The algorithm, developed for the Rubik's Cube, focuses on dividing up the main Rubik's Group into smaller and smaller subgroups, until arriving at the subgroup which contains only the identity move. The chain of subgroups are as follows;

$$G_0 =< \mathbf{U,D,F,B,R,L} >, \tag{98}$$
$$G_1 =< \mathbf{U2,D2,F,B,R,L} >, \tag{99}$$
$$G_2 =< \mathbf{U2,D2,F2,B2,R,L} >, \tag{100}$$
$$G_3 =< \mathbf{U2,D2,F2,B2,R2,L2} >, \tag{101}$$
$$G_4 =< e > . \tag{102}$$

The idea of the algorithm is that when you have a configuration, randomly selected from the orbit of the the solved configuration $(i_\sigma, i_{\mathbf{x}})$ under main Rubik's Group G_0, the first step is to use a combination of moves in G_0 to get to a configuration in the orbit of $(i_\sigma, i_{\mathbf{x}})$ under G_1.

We repeat this to get from a configuration in the orbit of $(i_\sigma, i_{\mathbf{x}})$ under subgroup G_{i+1}, to a configuration in the orbit of $(i_\sigma, i_{\mathbf{x}})$ under G_i until we are in a configuration in the orbit of $(i_\sigma, i_{\mathbf{x}})$ under G_4. Since G_4 contains only the identity element, this orbit contains only the solved configuration, $(i_\sigma, i_{\mathbf{x}})$ and we would have solved the Rubik's Cube.

To find the upper bound on God's Number, Morwen Thistlethwaite listed out, by hand, the **right cosets** of $G_{i+1}\backslash G_i$ and the number of moves to bring each coset into G_i. He did this for the entire chain of subgroups to find an upper bound of 52. This exact method was later performed by a computer to reach an upperbound of 45 on God's Number.

The handwritten look-up tables [2] used are lengthy, however the intuition of the technique is similar to the following example;

Example 6.1.1. Let the group $G = (\mathbb{Z}_8, +) =< 1 >$, and its chain of subgroups $H = (\mathbb{Z}_2, +) \cong (\{0, 4\}, +) =< 4 >$ and $I = \mathbb{Z}_0^+ = (\{0\}, +) =< 0 >$. The goal is to find the upper bound on the minimum number of +1s or -1s (moves) needed to get from any possible element of $\mathbb{Z}_8$ (valid configuration) to 0 (the solved configuration).

The right cosets of $H\backslash G$ are the following;

$$H = \{h + 0 : h \in H\} = \{0, 4\} \tag{103}$$
$$H + 1 = \{h + 1 : h \in H\} = \{1, 5\} \tag{104}$$
$$H + 2 = \{h + 2 : h \in H\} = \{2, 6\} \tag{105}$$
$$H + 3 = \{h + 3 : h \in H\} = \{3, 7\} \tag{106}$$

The right cosets of $I\backslash H$ are the following;

$$I = \{i + 0 : i \in H\} = \{0\} \tag{107}$$
$$I + 4 = \{i + 4 : i \in H\} = \{4\} \tag{108}$$

We see that to get from G to H takes at most 2 moves so the $eccentricity(H) = 2$ and to get from H to I takes at most 4 move, so the $eccentricity(I) = 4$. We therefore have that the upper bound on the $eccentricity(0)$ (gods number) is 6 compared to the actual number of 4 from Example 5.0.2.

6.2 Brute Force

The most straightforward approach to finding God's Number is to literally list out each and every possible configuration, their corresponding shortest move to get to it, and find the configuration that required the most number of moves to get to from a solved configuration. Which is why it is a brute force method.

This entails building the Cayley Graph of the group and using an algorithm to determine the longest shortest path originating from a solved configuration of the Rubik's Cube.

Definition 6.2.1. [11] Given a graph $G = (V, E)$ and a distinguished initial vertex $s \in V$, **Breadth-First Search** systematically explores the edges of G to "discover" every vertex that is reachable from s. It computes the depth (smallest number of edges) from s to each reachable vertex and produces a "breadth-first tree" with root s containing all reachable vertices. For any vertex v reachable from s, the path in the breadth-first tree from s to v corresponds to a "shortest path" from s to v in G (refer to page 532 of [11] for the pseudocode of the algorithm).

To do this, we alter a **Breadth-First Search** algorithm (Definition 6.2.1) to build the Breadth-First Cayley Graph so that the configurations of the shortest moves are first visited and any longer path to get to a same configuration can be discarded, as described in Algorithm 1.

We note that these discarded moves are the moves of the relation set which could be used to define the group structure.

Algorithm 1 Breadth-First Cayley Graph

```
while unexplored is not empty do
    procedure RECORD
        node ← next item from unexplored queue
        successors ← the successors of node using the basic moves
        for succ in successors do
            if the node succ hasn't been visited before then
                add succ to the unexplored queue and the visited list
```

7 Application to the Pocket Cube

In this section, we will see how the methods discussed in the previous section can be used to find God's number for the Pocket Cube. We will also analyse the algorithm used and compare the overall speedup gained after applying some optimisations to the algorithm.

7.1 Algorithm Analysis

When analysing algorithms we often talk about the worst possible case for the algorithm which incurs the longest run-time and largest memory usage. We call this the time and memory complexity of the algorithm. Formally we use the **asymptotic upper bound** denoted by **O-notation** to describe these notions.

Definition 7.1.1. [11] When we have an *asymptotic upper bound*, we use O-notation. For a given function $g(n)$, we denote by $O(g(n))$ (pronounced "big-oh of g of n") the set of functions

$$O(g(n)) = \{f(n) : \exists \text{ positive constants } c \text{ and } n_0 \text{ s.t } 0 \leq f(n) \leq cg(n), \forall n \geq n_0\}. \tag{109}$$

In order to build a Cayley Graph, we first initialise the *unexplored* queue with the initial node(s) (the solved configurations) and assign each of them with a depth of 0. Next, we initialise an empty hash table (a dictionary in python) to store the nodes which have been visited along with their depth, their parent node and the type of edge used to arrive at the node. Finally, we run Algorithm 1 until termination. It's easy to see that the loop-invariant of the algorithm is that the *unexplored* queue is not empty.

More specifically, in the case of the Pocket Group $\mathcal{P}$, we first need to define the moves which generate the group. By representing the configuration of a cube by a string of 16 digits, where the first 8 represent the positions of the cubies and the subsequent 8 represent this orientation, we can define the basic moves $\mathcal{B}$ of the Pocket Cube to alter the string appropriately, following Equations 56, 57, 58, 59, 60, 61 and Table 1.

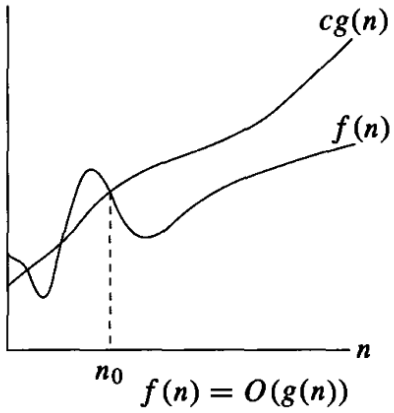

Figure 18: Intuition of O-notation
Source: [11]

On execution of the algorithm we see that on each iteration of the main loop, given by Algorithm 1, there is a for-loop which loops based on the number of basic moves (moves which count as 1 move) where $|\mathcal{B}|$ depends on the turn metric used. At the first iteration at depth 0, we would check the set conaining each an every initial solved configuration, $\mathcal{I}$, and apply the basic moves to each of them to get all the configurations at depth 1, giving us $|\mathcal{I}| \times |\mathcal{B}|$ nodes to repeat on in the next round to find nodes at depth 2. In the worst case scenario, we are checking $|\mathcal{B}|$ edges for each node at that depth. We repeat this until we have explored all nodes in the *unexplored* queue reaching depth $d = eccentricity(\mathcal{I})$. This algorithm is visualised in Figure 19

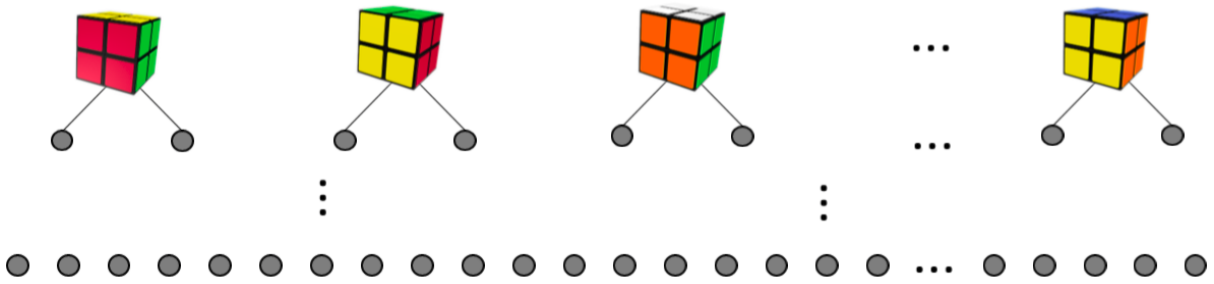

Figure 19: Simple Visualisation of the Algorithm on $\mathcal{P}$.

Therefore, the time complexity $= O(|\mathcal{I}||\mathcal{B}|^d) = O(|\mathcal{B}|^d)$ since $|\mathcal{I}|$ is constant. We also have that the *unexplored* array can, in the worst case, increase upto a memory complexity $= O(|\mathcal{B}|^d)$.

Now we have that we can run the algorithm using either the half-turn metric or the quater-turn metric, each giving different number of basic moves and depths to the Cayley Graph;

- Half-Turn Metric:
  - $|\mathcal{B}| = 18$,
  - d = 11,
  - Time & Memory Complexity $= O(18^{11})$,
- Quarter-Turn Metric:
  - $|\mathcal{B}| = 12$,
  - d = 14,

– Time & Memory Complexity = $O(12^{14})$.

Subsequently, running this algorithm on a single 2.6 GHz SandyBridge core with 4GB RAM, which can process on average 12,000 of the inner for-loops per second (to simplify the calculation assume that the time for memory access is linear with size of the array), would take using the:

- Half-Turn Metric;

$$\text{Time} = 18^{11}/12000 = 5,355,700,839.94s \approx 170 \text{ years}. \tag{110}$$

- Quarter-Turn Metric;

$$\text{Time} = 12^{14}/12000 = 106,993,205,379s \approx 3,400 \text{ years}. \tag{111}$$

Based on the time-complexity alone, this is already not even remotely feasible. Thus the Pocket Group $\mathcal{P}$ is too large to process using our algorithm. The main issue with the Pocket Group $\mathcal{P}$ is that there are multiple solved configurations which are basically spatial symmetries of each other. This means that the same sequence of moves applied to different solved configurations will arrive at different valid configurations. However, as proven in Section 4.2 we can simplify the Pocket Cube to remove these spatial symmetries giving us the simplified Pocket Group $\mathcal{Q}$.

Now we have that the simplified Pocket Group $\mathcal{Q}$ is much smaller than $\mathcal{P}$ and it follows that;

- Half-Turn Metric:
  - $|\mathcal{B}| = 9$,
  - d = 11,
  - Time & Memory Complexity = $O(9^{11})$,
- Quarter-Turn Metric:
  - $|\mathcal{B}| = 6$,
  - d = 14,
  - Time & Memory Complexity = $O(6^{14})$.

Subsequently, running this algorithm on the same architecture as before; a single 2.6 GHz SandyBridge core with 4GB RAM, which can process on average 12,000 of the inner for-loops per second; would take using the:

- Half-Turn Metric;

$$\text{Time} = 9^{11}/12000 = 2,615,088.30075s \approx 30 \text{ days}. \tag{112}$$

- Quarter-Turn Metric;

$$\text{Time} = 6^{14}/12000 = 6,530,347.008s \approx 75 \text{ days}. \tag{113}$$

The algorithm on $\mathcal{Q}$ runs $\mathbf{2048}\times$ faster than if it was run on $\mathcal{P}$ for the half-turn metric and $\mathbf{16,384}\times$ faster in the case of the quarter-turn metric. Keep in mind that this is the worst-case run-time analysis and doesn't consider any generator relations of the group. Ultimately, the generator relations would reduce the average branching factor, currently assumed to be the maximum branching factor $|\mathcal{B}|$.

Now we have that the simplified Pocket Group $\mathcal{Q}$ necessarily represents group $\mathcal{P}$ such that God's number isn't affected and is such a size that the Cayley Graph is computable.

7.2 Thistlethwaite's algorithm

As described in Section 6.1, Thistlethwaite's algorithm is a 4 part process. We can apply this to the Pocket Cube by building the Cayley Graphs associated with each right coset $G_{i+1}\backslash G_i$. We note, however, that in the case of running this on $\mathcal{P}$ we have that there is more than one solved configuration and so G_4 would be the group of solved configuration, which, in this case, would be $G_4 =< R_x, R_y, R_z >$.

To execute this we first initialise the *unexplored* list with the solved configurations; effectively setting the root nodes; then build the Cayley Graph of $G_4 \backslash G_3$. We note down the maximum depth of the tree from the roots. Next, we use the nodes from the coset as root nodes for the next Cayey Graph of $G_3 \backslash G_2$. We repeat this process for all cosets $G_{i+1} \backslash G_i$ until we have the depth of the cayley graph for all cosets. Finally we sum together all the depths to get the upper bound on God's number.

In practice, we use the simplified Pocket Group $\mathcal{Q}$ and have that the chain of subgroups are; $G_4 \leq G_3 \leq G_2 \leq G_1 \leq G_0$ where

$$G_0 =< \mathbf{U,\ F,\ R} > \tag{114}$$
$$G_1 =< \mathbf{U2,\ F,\ R} > \tag{115}$$
$$G_2 =< \mathbf{U2,\ F2,\ R} > \tag{116}$$
$$G_3 =< \mathbf{U2,\ F2,\ R2} > \tag{117}$$
$$G_4 =< e > . \tag{118}$$

Upon execution of the Thistlethwaite algorithm, we get the results in Table 3. The algorithm runs in 7255 seconds $\approx$ 2 hours.

Set of Cosets	**No of Cosets**	**Elements per Coset**	**Depth of Cayley Graph**
$G_4 \backslash G_3$	24	1	4
$G_3 \backslash G_2$	210	24	11
$G_2 \backslash G_1$	729	5040	9
$G_1 \backslash G_0$	1	3674160	0

Table 3: Results from Thistlethwaite's Algorithm

7.2.1 Conclusion

From here we can see that using Thistlethwaite's algorithm with the half-turn metric, we get an upper bound of $4 + 11 + 9 + 0 = 24$ on God's Number for the Pocket Cube.

We also see that there was only one right coset in $G_1 \backslash G_0$. This means that the set of generators of G_1, $\{\mathbf{U2,\ F,\ R}\}$ are sufficient to generate all possible configurations of the Pocket Cube.

Therefore, in actuality, Thistlethwaite's algorithm could have completed after finding the cosets $G_2 \backslash G_1$, which took only 2220 seconds = 37 minutes.

7.3 Brute Force

Now we use the brute force approach, described in Section 6.2, to find the exact God's number. Effectively, this is finding the depth of the Cayley Graph for the Pocket Group $\mathcal{P}$, however, since the group is too large to run the algorithm on, we use the simplified Pocket Group $\mathcal{Q}$ which also gives us God's number, as proven in Section 4.2.

Running the algorithm creates the Cayley Graph $\mathcal{C}_\mathcal{Q}$ of $\mathcal{Q}$. The algorithm took 2774 seconds $\approx$ 46 minutes to fully run. Table 4 shows the number of nodes at a particular depth of the $\mathcal{C}_\mathcal{Q}$ where each one represents a move which cannot be simplified further using the generator relations. There is no nodes at a depth greater than 11 so God's Number is 11 with the half-turn metric.

7.3.1 Generator Relations

We introduced in Section 6.2 that the cycles in the Cayley Graph of a group G define generator relations of he group. Using the function **store-generator-relations()** which is called when a previously encountered node is encountered again.

depth	Number of Nodes
0	1
1	9
2	54
3	321
4	1,847
5	9,992
6	50,136
7	227,536
8	870,072
9	1,887,748
10	623,800
11	2,644
Total	**3,674,160**

Table 4: Results from Brute Force Algorithm.

Algorithm 2 Breadth-First Cayley Graph with generator relations

```
while unexplored is not empty do
    procedure RECORD
        node ← next item from unexplored queue
        successors ← the successors of node using the basic moves
        for succ in successors do
            if the node succ hasn't been visited before then
                add succ to the unexplored queue and the visited list
            else
                store-generator-relations()
```

This means that there is already a shortest path $m_1 \in \mathcal{Q}$ to that node where $m_1 = a_1a_2...a_m$, however, a collision means that there is another path, $m_1 = m_2 = b_1b_2...b_n$ where $a, b \in \mathcal{B}$ and $m \leq n \in \mathbb{N}_0$, which would normally be discarded. We have 2 cases:

1. $a_1a_2...a_i = b_1b_2...b_i$ for some $i \in \mathbb{N}$ and so $a_{i+1}...a_m = b_{i+1}...b_n$ is a generator relation; or
2. there is no such $i \in \mathbb{N}$ such that $a_1a_2...a_i = b_1b_2...b_i$ and so $a_1a_2...a_m = b_1b_2...b_n$ is the generator relation.

Proposition 7.3.1. We have that the generator relation can only be a suffix of the move word m

Proof. Assume that the generator relation was the prefix $m_p = a_1a_2...a_i$ of the word move. By manner of the algorithm, the word move $a_1a_2...a_i$ would have encountered a collision and the path would have been discarded from the main search and so the move word would not have been searched, which is a contradiction. □

By implementing this in the Brute Force Algorithm, we find that there are 16,225,665 generator relations found when using the half-turn metric. Finding the independent set of generator relations is difficult.

However by reducing the number of basic moves to solely {**U, F, R**}, where $\mathbf{U}^2$ counts as 2 moves and the inverse $\mathbf{U}^3$ counts as 3 moves, the number of generator relations significantly reduces to 3,545,475.

7.3.2 Conclusion

The expected runtime of the algorithm, using the half-turn metric, was 30 days. The algorithm ran in 46 minutes. This is because the analysis previously done assumed that there were no generator relations

and at each depth of the graph the number of nodes increased exponentially, which is clearly not the case as seen in Table 4.

A careful analysis shows that the unexplored set in Algorithm 1 has each and every valid configuration of the cube in it once and only once. This means that for each node taken from the unexplored queue, we check $\mathcal{B}$ possible successors. Therefore we have that the time-complexity is $O(|\mathcal{B}|C)$ where C is the total number of configuration of the Pocket Cube.

Finally, we see that the generators of the group are useful to run the brute force algorithm of finding God's Number, however, the structure defined by the direct and semi-direct products were needed to conduct a proper analysis of the algorithm.

8 Discussion & Future Work

We have seen that in order to find God's Number for the Pocket Cube, we needed to understand the group structure very well in order to simplify it to a size that fits in the memory of a computer. For the case of the Rubik's Cube, very similar methods were used, but with very smart subgroups of the Rubik's cube, to split the group into cosets of a size that would fit on the memory of a computer. Interestingly, however, the method used to prove that God's Number for the Rubik's cube is 20 didn't use a brute force method. The details of how this was done is in the paper [15].

As of May 2019, God's Number for he 4x4x4 Rubik's Revenge Cube has not been found, however it is currently bounded below by 35 moves and above by 55 moves.

Looking back at how we analysed the algorithm initially, assuming that there were no generator relations, we can derive a generic formula for the lower bound of God's Number for any $n \times n \times n$ Rubik's Cube such that God Number is bounded below by $log_{|\mathcal{B}|}C$ where C is the number of configurations of the cube.

One last interesting and recent advancement into solving the Rubik's has been the implementation of a new machine learning technique called "autodidactic iteration" to solve the Rubik's Cube. Unlike anything that we have already done, it doen't take any prior knowledge about the group structure to find a non-optimal but good solution to a scrambled configuration [18]. Perhaps we will see in the near future the answers to God's Number for larger cubes, without knowing how we actually go the answer.

References

[1] D. Singmaster. *Notes on Rubik's magic cube*. Enslow Publishers, 1981. ISBN: 9780894900433. URL: https://books.google.co.uk/books?id=UGIPAQAAMAAJ.

[2] M. Thistlethwaite. *Thistlethwaite's 52-move algorithm*. 1982. URL: https://www.jaapsch.net/puzzles/thistle.htm.

[3] Herbert Kociemba. *Two-Phase Algorithm Details*. 1992. URL: http://kociemba.org/math/imptwophase.htm.

[4] Michael Reid. *Superflip requires 20 face turns*. 1995. URL: https://www.cs.brandeis.edu/~storer/JimPuzzles/RUBIK/Rubik3x3x3/READING/SuperflipRequires20FaceTurns.pdf.

[5] John F. Humphreys. *A Course in Group Theory*. Oxford University Press, 1996. ISBN: 9780198534532. URL: https://books.google.co.uk/books/about/A_Course_in_Group_Theory.html?id=2jBqvVb0Q-AC&redir_esc=y.

[6] David Joyner. *Adventures in group theory : Rubik's Cube, Merlin's machine, and other mathematical toys*. Johns Hopkins University Press, 2002. ISBN: 9780801869471. URL: https://books.google.co.uk/books?id=iM0fco-_Ri8C.

[7] Janet Chen. *Group Theory and the Rubik's Cube*. 2004. URL: http://www.math.harvard.edu/~jjchen/docs/Group%5C%20Theory%5C%20and%5C%20the%5C%20Rubik%5C%27s%5C%20Cube.pdf.

[8] Unidentified Free Artist. *Rubik Cubism*. 2005. URL: https://www.space-invaders.com/post/rubikcubism/.

[9] Daniel Bump and Daniel Auerbach. *Unravelling the (miniature) Rubik's Cube through its Cayley Graph*. 2006. URL: http://sporadic.stanford.edu/bump/match/morepolished.pdf.

[10] Tom Davis. *Group Theory via Rubik's Cube*. 2006. URL: http://www.geometer.org/rubik/group.pdf.

[11] Thomas H. Cormen [and Others]. *Introduction to Algorithms*. MIT Press, 2009. ISBN: 9781628709131. URL: https://www-dawsonera-com.bris.idm.oclc.org/abstract/9780262270830.

[12] H.E. Rose. *A Course on Finite Groups*. Springer, 2009. ISBN: 9781848828896. URL: https://www.springer.com/gb/book/9781848828889.

[13] Charles C. Pinter. *A Book of Abstract Algebra*. Dover Publications, 2010. ISBN: 9780486474175. URL: https://books.google.co.uk/books?id=PmzjBwAAQBAJ.

[14] Morley Davidson Tomas Rokicki Herbert Kociemba and John Dethrudge. *God's Number is 20*. 2013. URL: https://www.cube20.org.

[15] Morley Davidson Tomas Rokicki Herbert Kociemba and John Dethrudge. *The Diameter of the Rubik's Cube Group is Twenty*. 2013. URL: https://tomas.rokicki.com/rubik20.pdf.

[16] Professor. Rickard. *MATH10005*. 2016. URL: https://www.bris.ac.uk/unit-programme-catalogue/UnitDetails.jsa?ayrCode=16%5C%2F17&unitCode=MATH10005.

[17] Julia Wolf. *MATH20002*. 2017. URL: http://www.juliawolf.org/teaching/MATH20002.shtml.

[18] Emerging Technology from the arXiv. *A machine has figured out Rubik's Cube all by itself*. 2018. URL: https://www.technologyreview.com/s/611281/a-machine-has-figured-out-rubiks-cube-all-by-itself/?utm_source=facebook.com&utm_campaign=owned_social&utm_medium=social&fbclid=IwAR335BT3yPIxVqdZyEETqKs70K1Uo-w_0b75swGESOaWtkJnBl8FoXI8fu8.

[19] Tim Burness. *MATH33300*. 2018. URL: https://www.bristol.ac.uk/maths/undergraduate/units1819/levelh6units/group-theory-math33300/.

[20] Bryce Springfield. *Cube Turn Metrics*. 2018. URL: https://www.speedsolving.com/wiki/index.php/Metric.

[21] Wikipedia Contributors. *Ideal Toy Company*. URL: https://en.wikipedia.org/wiki/Ideal_Toy_Company.

[22] Grubiks.com. *Mini Rubik's Cube (2x2x2)*. URL: https://www.grubiks.com/puzzles/rubiks-mini-cube-2x2x2/.

[23] Office of Media Relations. *Role of Larry Nichols '58 in Inventing Famous Toy Recalled*. URL: https://www.depauw.edu/news-media/latest-news/details/31162/.

[24] Weburbanist Steve. *Rubik Cubism*. URL: https://weburbanist.com/2010/06/27/i-rubikcubist-30-twisted-works-of-rubiks-cube-art/.