Group Theory and its Application to the Rubik's Cube

Christopher Hickey

April 2014

Abstract

This essay concerns itself with the concept of groups and how they are useful in proving several properties of the 2x2x2 Rubik's Cube. I will first find several groups of interest, before using them to prove properties such as the number of solvable cube configurations.

Contents

1 A Brief Introduction to Group Theory

1.1 Defining the Group and Group Properties

Before we define a group, we must first define various important concepts.

Definition 1.1. *A **set** is a collection of distinct elements and an **n-tuple** is an ordered set containing n elements. Sets usually have curly braces, '{}', whilst for tuples we use regular brackets, '()'.*

Definition 1.2. *A **binary operator** on a set A is a map $\bullet : A \times A \mapsto A$ where $A \times A$ is the set of all 2-tuples (a, b) with $a, b \in A$. We often write $\bullet(a, b)$ as $a \bullet b$ or just ab.*

With these definitions we can now define the group.

Definition 1.3. *A **group** is a set, G, with an operation, $\bullet$, that satisfies these 4 conditions, called the Group Axioms;*

1. *Closure*
   $a \bullet b \in G \quad \forall a, b \in G$ *(i.e. $\bullet$ is a binary operation)*
2. *Associativity*
   $(a \bullet b) \bullet c = a \bullet (b \bullet c) \quad \forall a, b, c \in G$
3. *Existence of Identity Element*
   $\exists e \in G \quad s.t. \quad \forall a \in G \quad a \bullet e = e \bullet a = a$
4. *Existence of Inverse Element*
   $\exists a' \in G \quad s.t. \quad \forall a \in G \quad a \bullet a' = a' \bullet a = e$ *(a' is called the inverse of a)*

Remark 1.1. *We denote the group formed from a set G and binary operator $\bullet$ by $(G, \bullet)$. We write $g \bullet g$ as g^2 and similarly write $g \bullet g \bullet \ldots \bullet g$, where we use $\bullet$ $n - 1$ times, as g^n. This shorthand becomes useful in defining Rubik's Cube move sequences.*

Definition 1.4. *The **order of a group**, G, is the number of elements in the group, it is written as $|G|$. The **order of an element**, $g \in G$, is the smallest positive integer, n, s.t. $g^n = e$, the identity element of G. We write $|g| = n$.*

We next define a subgroup. Subgroups are useful as they allow for a greater understanding of the binary operator on a group [**1,§5**].

Definition 1.5. *A subset, H, of a group, $(G, \bullet)$, is a **subgroup** if $(H, \bullet)$ forms a group.*

We use subgroups to define what a generating set of a group is. Generating sets can be used to gain more understanding of the symmetries and patterns in a large order group [**2**].

Definition 1.6. *Let S be a subset of a group G.*
*The **subgroup generated by** S, $< S >$ is the smallest subgroup of G containing every element of S (i.e. $< S >$ is the subgroup of elements of G that can be expressed as the finite product of elements of $< S >$). The **Generating Set** of a group is the smallest set, S, such that $< S >= G$.*

With these basic definitions on the group, we can get into the much more interesting group theory.

1.2 Functions Involving Groups

We will be looking to define functions in the next section so as to understand how moves affect the configuration of the Rubik's Cube. But first there is a very important definition that allows us to categorise types of functions.

Definition 1.7. *For the function $f : A \to B$*
*f is **injective** if $\forall a, a' \in A, \quad f(a) = f(a') \implies a = a'$.*
*f is **surjective** if $\forall b \in B, \exists a \in A, \quad f(a) = b$.*
*f is **bijective** if it is surjective and injective.*

1.2.1 Permutations

The first of these functions is not on a group, but is very important within group theory. It involves a function which rearranges the elements of a set.

Definition 1.8. *A **permutation** of A is a bijective function $\rho : A \to A$*

We can compose permutations of the same set, and use this as the binary operator to define a group. We call the set of all permutations of A with the "composition of functions" binary operator (denoted $\circ$, so for permutations ϕ, ψ we have that $\phi \circ \psi = \phi(\psi)$) the symmetric group of A, S_A.

There are many ways to denote how a permutation affects a group, the way we will use is cycle notation. In cycle notation a permutation would be written by the 'cycle' created by repeatedly performing the permutation on an element. A permutation, ϕ, on the set $B = \{b_1, 2, 3, \dots, b_n\}$ would be written as a collection of cycles, $(b_1, b_2, \dots b_k)$ with $1 \leq k \leq n$ where $\phi(b_i) = b_{i+1}$ for $i \in [1, 2, \dots, k-1]$ and $\phi(b_k) = b_1$.

Proposition 1.1. *Every permutation can be written as a composition of permutations of cycle length 2, called transpositions.*

Proof. Consider the above cycle of length k, $(b_1, b_2, \dots b_k)$. This can be rewritten as

$$(b_1, b_k)(b_1, b_{k-1})...(b_1, b_2)$$

It follows that all cycles can therefore be written as compositions of transpositions. □

1.2.2 Homomorphisms

The next function we define is called a homomorphism. It provides a way to relate the binary operations of two groups.

Definition 1.9. *A **homomorphism**, ϕ, is a function that maps a group $(G, \bullet)$ to a group $(H, *)$ and has the following property $\forall a, b \in G$;*

$$\phi(a \bullet b) = \phi(a) * \phi(b)$$

*From homomorphisms we also get two other classes of functions; **isomorphisms** are bijective homomorphisms, and **automorphisms** are isomorphisms that map groups onto themselves.*

As you can imagine, these are a very useful collection of functions. They preserve group structure as $\phi : G \to G$ can easily be shown that ϕ preserves the identity and inverses **[1,pp139-140]**.

We will see later they are also useful in the case where we have a homomorphism $\phi : (G, \bullet) \to (H, *)$ and the group $(G, \bullet)$ which is generated by the subset S as

$$\begin{aligned}\forall g \in G \text{ with } g = s_1 \bullet s_2 \bullet \ldots \bullet s_n \text{ for some } s_1, s_2, \ldots s_n \in S,\\ \phi(g) &= \phi(s_1 \bullet s_2 \bullet \ldots \bullet s_n)\\ &= \phi(s_1) * \phi(s_2) * \ldots * \phi(s_n)\end{aligned}$$

So if ϕ was a complex function and we wanted to find $\phi(g)$ for many values of g (more than $|S|$), we would only have to calculate $\phi(s)\ \forall s \in S$.

Definition 1.10. *The* ***automorphism group*** *of G is the set of all automorphisms of the group G, it is denoted $Aut(G)$.*

For the groups we will look at $Aut(G)$ is the symmetry group of G, as the only automorphisms on the sets we will look at will be permutations. In this essay we will often write $Aut(G)$ instead of S_G to fit in with later definitions.

1.2.3 Group Actions

A group action allows us to investigate how the symmetries of a group can affect the elements of a set. This means we can get a much clearer description of the symmetry of an object. For example we can explore the consequences of the symmetry group of a polyhedron acting on the set of its vertices or edges [**3**].

Definition 1.11. *A* ***(left) group action*** *of a group G on a set X is a function $\phi : G \times X \to X$ with the following properties $\forall x \in X$;*

1. *$\phi(gh, x) = \phi(g, \phi(h, x))\ \forall g, h \in G$*
2. *$\phi(e, x) = x$ for x the identity of G*

Often we write $\phi_g(x)$ to represent $\phi(g, x)$.
Similarly we have a ***right group action*** *by redefining the function ϕ to be from $\phi' : X \times G \to X$ and altering the ordering of properties appropriately.*

We will next use the following propositions from *On Rubik's Cube* [**4,§1.2.5**].

Lemma 1.2. *Let $(G, \circ)$ be a group of permutations and X a set with a group action $\phi : G \times X \to X$. Define for fixed $g \in (G, \circ)$ the function $\phi_g : X \to X$ where $\phi_g = \phi(g, x)\ \forall x \in X$. Then ϕ_g is a permutation.*

Proof. The proof for this has been omitted but can be found in On Rubik's Cube [**4,Proposition 1.2.37**]. □

This lemma leads to a proposition that allows us to connect the ideas of group actions and homomorphisms.

Proposition 1.3. *Let $\phi : G \times X \to X$ be a group action on the group $(G, \circ)$ and set X and now define $f : (G, \circ) \to Aut(X)$ where $f(g) = \phi_g$, the group action from above. Then f is a homomorphism.*

Proof. Consider $g, h \in (G, \circ)$ and $x \in X$. To show f is a homomorphism we must show $f(g \circ h) = f(g) \circ f(h)$.

$$\begin{aligned} f(g \circ h)(x) &= \phi(g \circ h, x) \\ &= \phi(g, \phi(h, x)) \\ &= (\phi_g \circ \phi_h)(x) \\ &= (f(g) \circ f(h))(x) \end{aligned}$$

This holds $\forall x \in X$ therefore f is a homomorphism. □

1.2.4 Semi-Direct Product

Our final group function we will look at is more abstract than the previous three. First we will introduce the idea of direct product.

Definition 1.12. *The* ***direct product*** *of $G_1, G_2, \ldots, G_n$ is $G_1 \times G_2 \times \ldots \times G_n$, where $G_1, G_2, \ldots, G_n$ are groups, and $G_1 \times G_2 \times \ldots \times G_n$ is a set of all n-tuples of the form $(g_1, g_2, \ldots, g_n)$ with $g_i \in G_i$ $\forall i \in [1, 2, \ldots, n]$.*

From *On Rubik's Cube* [**4, Proposition 1.2.49**] we see that this set forms a group, the proof is omitted from the essay due to length.
We can now begin to think about semi-direct product, which is a more general idea than direct product. There are two ways to approach semi-direct product: outer semi-direct product which we will define next, and inner semi-direct product which is beyond the scope of this essay. As we will only be using outer semi-direct product, we will refer to it as semi-direct product from here on in.

Definition 1.13. *Let $(H, \star)$ and $(G, \bullet)$ be groups, with a homomorphism $\phi : H \to Aut(G)$ where we write for $h \in H$ $\phi(h) = \phi_h$. We define a set $G \rtimes_\phi H$ as the cartesian product $G \times H$. The* ***semi-direct product*** *is this set with the operation $* : (G \rtimes_\phi H) \times (G \rtimes_\phi H) \to (G \rtimes_\phi H)$ where*

$$(g_1, h_1) * (g_2, h_2) = (g_1 \bullet \phi_{h_1}(g_2), h_1 \star h_2)$$

for any $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Theorem 1.4. *The semi-direct product as written above forms a group.*

Proof. We need to show this set $G \rtimes_\phi H$ with the operation $*$ follows the 4 group axioms.

1. Closure
   As $(H, \star)$ is a group, it is clear that $h_1 \star h_2 \in H$. We next need to show $g_1 \bullet \phi_{h_1}(g_2) \in G$ which follows from $\phi_{h_1} \in Aut(G)$. Hence $*$ is closed, and therefore is a binary operation.

2. Associativity
   We want to show $(g_1, h_1) * ((g_2, h_2) * (g_3, h_3)) = ((g_1, h_1) * (g_2, h_2)) * (g_3, h_3)$

$$\begin{aligned} (g_1, h_1) * ((g_2, h_2) * (g_3, h_3)) &= (g_1, h_1) * (g_2 \bullet \phi_{h_2}(g_3), h_2 \star h_3) \\ &= (g_1 \bullet \phi_{h_1}((g_2) \bullet \phi_{h_2}(g_3)), h_1 \star (h_2 \star h_3)) \\ &= ((g_1 \bullet \phi_{h_1}(g_2)) \bullet \phi_{h_1 \star h_2}(g_3), (h_1 \star h_2) \star h_3) \\ &= (g_1 \bullet \phi_{h_1}(g_2), h_1 \star h_2) * (g_3, h_3) \\ &= ((g_1, h_1) * (g_2, h_2)) * (g_3, h_3) \end{aligned}$$

3. Existence of Identity
   We need to show that the identity is (e_g, e_h) where e_g and e_h are the respective identities of G and H. Clearly $\phi_{e_h} = e_{Aut(G)}$ so $\phi_{e_h}(g) = g \ \forall g \in G$. Since ϕ is a homomorphism we have $\phi_h e_g = e_g$, therefore we get that

$$(e_g, e_h) * (g, h) = (e_g \bullet \phi_{e_h}(g), e_h \star h) = (g, h)$$
$$(g, h) * (e_g, e_h) = (g \bullet \phi_h(e_g), h \star e_h) = (g, h)$$

4. Existence of Inverse
   We need a element (g', h') so that $(g', h') * (g, h) = (g, h) * (g', h') = (e_g, e_h)$. We know;

$$(g', h') * (g, h) = (g' \bullet \phi_{h'}(g), h' \star h) \tag{1}$$
$$(g, h) * (g', h') = (g \bullet \phi_h(g'), h \star h') \tag{2}$$

   We can see that for $h' \star h$ to be e_h we must have that h' is the inverse of h, h^{-1}. We next get that $g \bullet \phi_h(g') = e_g$ means that $g^{-1} = \phi_h(g')$ so $g' = \phi_h^{-1}(g^{-1})$. We can see this is the inverse by using that ϕ is a homomorphism and looking at equations (1) and (2):

$$(\phi_h^{-1}(g^{-1}), h^{-1}) * (g, h) = (\phi_h^{-1}(g^{-1}) \bullet \phi_{h^{-1}}(g), h^{-1} \star h) = (e_g, e_h)$$
$$(g, h) * (\phi_h^{-1}(g^{-1}), h^{-1}) = (g \bullet \phi_h(\phi_h^{-1}(g^{-1})), h \star h^{-1}) = (e_g, e_h)$$

□

Now we know this we can find the order of a semi-direct product.

Proposition 1.5. *The order of the semi-direct product $G \rtimes_\phi H$ as above to be $|G||H|$.*

Proof. This follows from the fact that for (g, h) there are $|G|$ different possible values of g and $|H|$ different possible values of h. Hence there are $|G||H|$ different possible values of (g, h). □

2 The Rubik's Cube Groups

In this chapter we will use group theory to prove some basic properties of the cube. We will create 2 groups, the first, $\mathcal{S}$, will be the group of finite move sequences, the second, $\mathcal{R}$ will be the group representing solvable configurations of the cube.

Firstly, we will define some notation[**5,§3.1**]. The 2x2x2 cube, also known as 2-Cube, is made up of 8 individual cubes, called cubies, denoted by c_i. Cubicles are the area cubies can be located, they are fixed reference points, defined by face name. We denote cubicles by the faces that cover them, for example, UFR, which is the cubicle formed by the shared corner of the up, front, and right faces. Figure 1 shows the notation on a solved cube. The following sets and tuples are how we will mathematically represent these aspects;

C $= \{c_1, c_2, \dots, c_8\}$, the set of all cubies.

A $= (ulb, ubr, urf, ufl, dlf, dbl, dbr, drf)$, the tuple of all cubicles.

C_A $= (c_1, c_2, \dots, c_8)$, the tuple of all cubies, which with A can tell us the exact position of each cubie.

Θ $= (\theta_1, \theta_2, \dots, \theta_8)$ the tuple of cubie orientations where θ_i represents the orientation of the cubie in A_i.

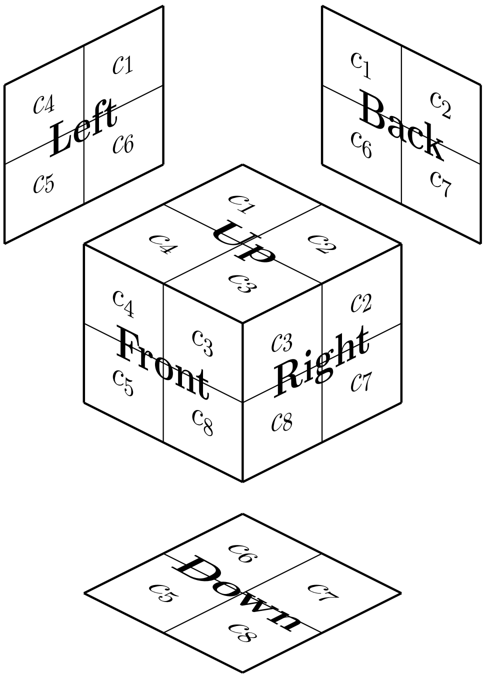

Figure 1: Whilst cubies can move, the names of the faces are fixed.

We can think of a move as a permutation of cubies from one cubicle to another. In the next section we hope to create a function (or functions) that gives us this permutation given any move sequence in $\mathcal{S}$.

2.1 Moves on the Cube

A move sequence on the cube can be split into a collection of individual 90° clockwise rotations performed on the 4 cubicles that make up a particular face. We will use the Singmaster Notation for the 3x3x3 Rubik's Cube (3-Cube) [**6,p8**] as this is the most common, and will allow us to see the relationship between the 2-Cube and 3-Cube. The moves are defined as follows (from the point of view of the face being moved):

L Rotate Left face 90° clockwise.

B Rotate Back face 90° clockwise.

U Rotate Up face 90° clockwise.

F Rotate Front face 90° clockwise.

R Rotate Right face 90° clockwise.

D Rotate Down face 90° clockwise.

We denote the set of moves $\{L, F, B, R, U, D\}$ by $\mathbb{M}$ and we define a finite move sequence to be some finite combination of elements of $\mathbb{M}$. For example, BUR represents performing the move B, U and then R. We will call the set of all finite move sequences $\mathbb{S}$ and define $\circ : \mathbb{S} \times \mathbb{S} \to \mathbb{S}$ where, for $M_1, M_2 \in \mathbb{S}$, $\circ(M_1, M_2)$ is the move sequence formed by performing M_1 followed by M_2. We call $\circ$ the concatenation operator, and usually write $M_1 M_2$ or $M_1 \circ M_2$ instead of $\circ(M_1, M_2)$

We can now define the first group, $\mathcal{S}$, formed from $\mathbb{S}$ with $\circ$.

Theorem 2.1. $(\mathbb{S}, \circ)$ *forms a group.*

Proof. To prove this, we simply show it follows the 4 group axioms.

1. Closure
   The group is closed, as a concatenation of 2 finite sequences is a finite sequence in itself, so must be in $\mathbb{S}$.

2. Associative
   Consider 3 finite sequences of moves M_1, M_2 and M_3. We need to check whether $M_1 \circ (M_2 \circ M_3) = (M_1 \circ M_2) \circ M_3$ is true. By evaluation we know from the definition that $M_1 \circ (M_2 \circ M_3)$ means performing M_1 followed by M_2 and M_3 and $(M_1 \circ M_2) \circ M_3$ means performing M_1 then M_2 all followed by M_3, clearly these are equivalent.

3. Existence of an Identity
   The empty sequence, e, is the sequence containing no moves, so $S_1 \circ e = e \circ S_1 = S_1 \quad \forall S_1 \in (\mathbb{S}, \circ)$, hence e is the identity element.

4. Existence of an Inverse
   Define $L^{-1}, B^{-1}, U^{-1}, F^{-1}, R^{-1}$ and D^{-1} as the moves L,B,U,F,R and D each performed three times respectively. Then the inverse of a sequence will be the moves in the sequence performed in the opposite order and replaced with the individual moves inverse. □

This group will be useful as we can now examine what moves sequences do to the position and orientations of cubies, but before this we will prove a simple but useful theorem.

Theorem 2.2. *The elements in* $\mathbb{M}$ *generate* $\mathcal{S}$.

Proof. There are only 6 possible individual moves one can perform on the cube, the elements $\mathbb{M}$. Therefore all sequences of moves will be elements of $\mathbb{M}$. □

2.2 Configuration: Position and Orientation.

Each time we perform a move on the cube the cubies position and orientation changes in some way. We will now begin to look into how to convey these changes mathematically.

2.2.1 Position

C_A tells us which cubies are in which cubicle, in the above example we can see c_2 is in the cubicle ubr. C_A allows us to keep track of the positions of the cubies relative to the fixed cubicles. To create ψ we must look to the concept of group actions and define $\phi : \mathcal{S} \times C \to C$ where $\phi(M, c_i) = c_j$ for some $M \in \mathcal{S}, c_i, c_j \in C$. ϕ returns the cubie, c_j, that, as a result of the move M, is in the cubicle c_i was in.

Theorem 2.3. *ϕ is a group action.*

Proof. Using the definition, we can say ϕ is a group action if;

1. $\phi(M_1 \circ M_2, c_i) = \phi(M_2, \phi(M_1, c_i)) \quad \forall M_1, M_2 \in \mathcal{S}, \quad c_i \in C$
   So $\phi(M_1 \circ M_2, c_i)$ would give us the $c_j \in C$ resulting from performing M_1 then M_2 on c_i. This is equivalent to performing M_1 on c_i then M_2 on the result, by definition of the concatenation operator.

2. $\phi(e, c_i) = c_i \quad \forall c_i \in C$
   for $c_i \in C \quad \phi(e, c_i) = ec_i = c_i$ as e doesn't move cubies. □

We can now define a permutation $\phi_M : C \to C$ with $\phi_M(c_i) = \phi(M, c_i) = c_j$. We use this permutation to observe how C_A changes after the move M, with C_A starting as $\{c_1, \dots, c_8\}$ and then being permuted to $\{\phi_M(c_1), \dots, \phi_M(c_8)\}$. We can represent these permutations as elements of $Aut(C_A)$, the symmetry group of C. We can define $\psi : \mathcal{S} \to Aut(C_A)$ where $\psi(M) = \phi_M$ performed on each element on C_A, therefore by proposition 1.3 we can see that ψ is a homomorphism.

This means if we have a move sequence, AB, with A and B arbitrary elements of $\mathbb{M}$, by using the definition of homomorphism we get $\psi(A \circ B) = \psi(A)\psi(B)$. So all we need to do to explain how any sequence in $\mathcal{S}$ affects the cubies is to define $\psi(m)\ \forall m \in \mathbb{M}$ as $\mathbb{M}$ generates $\mathcal{S}$;

$$\psi(L) = (c_1, c_4, c_5, c_6) \qquad \psi(F) = (c_3, c_8, c_5, c_4)$$

$$\psi(B) = (c_1, c_6, c_7, c_2) \qquad \psi(R) = (c_2, c_7, c_8, c_3)$$

$$\psi(U) = (c_1, c_2, c_3, c_4) \qquad \psi(D) = (c_5, c_8, c_7, c_6)$$

Example 2.1. *Consider the move sequence UBL;*

$$\begin{aligned} \psi(UBL) &= \psi(U)\psi(B)\psi(L) = & (c_1, c_2, c_3, c_4)(c_1, c_6, c_7, c_2)(c_1, c_4, c_5, c_6) \\ & = & (c_1, c_4)(c_2, c_3, c_5, c_6, c_7) \end{aligned}$$

As you can see, this move sequence swaps the two cubies c_1 and c_4, and cycles the c_2, c_3, c_5, c_6 and c_7 cubies.

Remark 2.1. *The above example shows that ψ is surjective, i.e. that it maps to every permutation of C. We can see this, as if you repeated UBL 5 times, the only change would be a transposition of c_1 and c_4, so by symmetry, using this move we can transpose any 2 cubies (by using $(URB)^5$, for example, which would swap c_2 and c_1). By Proposition 1.1, we know that every permutation can be written as a product of transpositions of 2 elements, so we can hence have any permutation of C.*

So we have a function that we can use to find the effects of moves on position, next we must do the same for orientation. This we will be considerably more complicated, as we do not yet have a way to define orientation.

2.2.2 Orientation

To mathematically represent the orientation of a cubie we look back to the tuple defined earlier,

$$\Theta = (\theta_1, \theta_2, \dots, \theta_8)$$

Each cubie can be orientated in 3 different ways, therefore we can say $\theta_i \in \{0, 1, 2\}$. If you imagine a cross drawn on the up face of each of the cubies on the upper half of the cube, and drawn on the down face of the

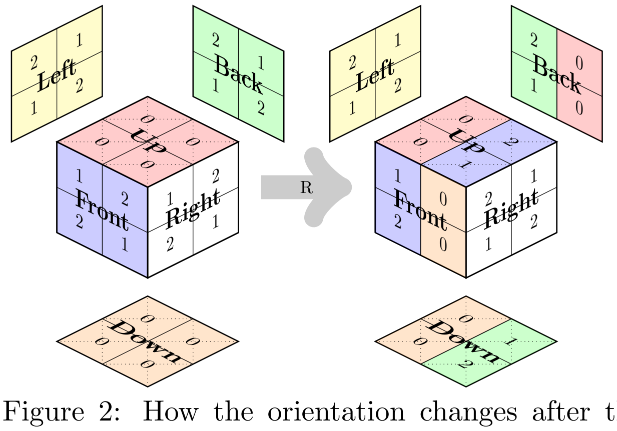

Figure 2: How the orientation changes after the move 'R'. Notice $\Theta_{before} = (0,0,0,0,0,0,0,0)$ and $\Theta_{after} = (0,2,1,0,0,0,1,2)$. (Colours added to indicate move).

other cubies. We can give θ_i a value based on how many clockwise 120° rotations it takes to get that c_i back to having the cross in the up or down face. The orientations of the solved cube are shown in Figure 2. We call the set of all possible orientations of the cube $\mathbb{O}$. As a cubie that is in the correct orientation is equivalent to a cubie that is 3 rotations away, we can say θ_i is in a group under addition modulo 3, $\mathbb{Z}/3\mathbb{Z}$. The group formed by $\mathbb{O}$ under addition modulo 3 is $(\mathbb{Z}/3\mathbb{Z})^8$.

Each time a move is performed, the positions of the cubes change, so the challenge here is keeping account of which cubies have which orientations. We need to permute the elements of $\Theta \in (\mathbb{Z}/3\mathbb{Z})^8$ using the permutations defined by ψ. Consider the effects of two sequences S_1, $S_2 \in \mathbb{S}$ which have the following effect on the solved cube:

S_1 cubies permuted $\psi_1 = \psi(S_1) \in Aut(C_A)$, cubies orientated $\Theta_1 \in \mathbb{Z}/3\mathbb{Z}$

S_2 cubies permuted $\psi_2 = \psi(S_2) \in Aut(C_A)$, cubies orientated $\Theta_2 \in \mathbb{Z}/3\mathbb{Z}$

So if we performed S_1 on the solved cube we would get a cube with its corners positioned by $\psi_1 C$ and the orientation of the cubies being Θ_1. If we then performed S_2, the cubies positions change by ψ_2. As the cubies have moved, this means we will have to change the ordering of the orientation tuple. To do this we will create a homomorphism $f : Aut(C_A) \to Aut((\mathbb{Z}/3\mathbb{Z})^8)$, where for $\psi \in Aut(C_A)$ permutes elements of C_A exactly as $f(\psi) \in Aut((\mathbb{Z}/3\mathbb{Z})^8)$ does in $(\mathbb{Z}/3\mathbb{Z})^8$. So we can describe the cubie orientation resulting from $S_1 \circ S_2$ performed on the solved cube as $\Theta_2 + f(\psi_2)\Theta_1$. The next logical step would be to describe how the elements of $\mathbb{M}$ affect orientation of the solved cube, because $\mathbb{M}$ generates $\mathcal{S}$, so we could then find out how any move sequence affects orientation. We can find the orientations resulting from the elements of $\mathbb{M}$ by inspection:

Θ_L $(1, 0, 0, 2, 1, 2, 0, 0)$	Θ_F $(0, 0, 2, 1, 2, 0, 0, 1)$
Θ_B $(2, 1, 0, 0, 0, 1, 2, 0)$	Θ_R $(0, 2, 1, 0, 0, 0, 1, 2)$
Θ_U $(0, 0, 0, 0, 0, 0, 0, 0)$	Θ_D $(0, 0, 0, 0, 0, 0, 0, 0)$

2.2.3 Configuration

Using what we now know about orientation and position of cubies, we can define a way to describe the configuration of the cube using a tuple. We define this tuple (C_A, Θ) where Θ tells us the orientation of the cubie in $c_i \in C_A$. The configuration of the solved cube is $((c_1, \ldots, c_8), (0, \ldots, 0))$, as each cubie is in its original cubicle, and all cubies are in the right position. We next have to figure out a way to find out whether this configuration is solvable. For the 2-cube, we know that any C_A is possible, as the function ψ is surjective. However, for orientations, looking at our values for Θ with respect to the generating moves, we can begin to form a theorem based on the fact the group is under addition modulo 3.

Theorem 2.4. *The cube is only solvable if* $\sum_{i=1}^{8} \theta_i = 0 \mod 3$

Proof. We will now perform induction by showing that the sum of the orientations after n moves (of $\mathbb{M}$) from a solved cube is $0 \mod 3$.
Firstly, consider $\Theta_m = \{\theta_{1_m}, \theta_{2_m}, \ldots, \theta_{8_m}\}$ for $m \in \mathbb{M}$. $\sum_{i=1}^{8} \theta_{i_m} = 0 \mod 3$ by inspection $\forall m \in \mathbb{M}$. So it is true for $n = 1$.
For $n = k$, M_k is any sequence of k arbitrary moves. Let the orientation after this move sequence be $\Theta_{M_k} = \{\theta_{M_{k_1}}, \ldots, \theta_{m_{k_8}}\}$ and assume $\sum_{i=1}^{8} \theta_{M_{k_i}} = 0 \mod 3$.
Now for $n = k+1$ consider performing another arbitrary move, $x \in \mathbb{M}$ which permutes the cubies

by some $\psi_x \in S_8$. Let the orientation after performing n be defined as $\Theta_x = \{\theta_{x_1}, \ldots, \theta_{x_8}\}$. From before, we found out that the orientation after performing M_k then x we have

$$\Theta_{M_k \circ x} = \Theta(x) + f(\psi_x)\Theta(M_k)$$

Now, clearly $f(\psi_x)\Theta(M_k)$ will not change the sum of the elements of $\Theta(M_k)$, as it just rearranges them. $\Theta(x)$ is just another element of $\mathbb{M}$, and we know this means that $\sum_{i=1}^{8} \theta_{x_i} = 0 \mod 3$. So $\sum_{i=1}^{8} \theta_{M_k \circ x_i} = 0$.
Therefore by induction we have that after a move in $\mathcal{S}$ the orientation of the cubies must sum to 0 mod 3. Hence the cube is only solvable when $\sum_{i=1}^{8} \theta_i = 0 \mod 3$. □

Hence we know that we will only ever be interested in $\Theta \in (\mathbb{Z}/3\mathbb{Z})^8$ such that $\sum_{i=1}^{8} \theta_i = 0$ mod 3, so we will now create a subset of $(\mathbb{Z}/3\mathbb{Z})^8$ where this is always true, $(\mathbb{Z}/3\mathbb{Z})^8_\star = \{\Theta \in (\mathbb{Z}/3\mathbb{Z})^8 : \sum_{i=1}^{8} \theta_i = 0 \mod 3\}$.

2.3 $\mathcal{R}$

Using what we now have, and with our way to check whether the cube is solvable, we can define the set of solvable configurations as $\{(x, y) : x \in C_A, y \in (\mathbb{Z}/3\mathbb{Z})^8_\star\}$. But we are looking to define a group, not a set, for $\mathcal{R}$ we will introduce a new way to think of cube configuration. $\mathcal{R}$ will be the group of moves required to reach each individual configuration of the cube.

2.3.1 Configuration and Semi-Direct Product

We will first define the configuration of the cube again, this time as a move acted on the solved cube which takes us to that configuration. However, we do not need to know the move as a sequence of elements of $\mathbb{M}$, all we need to know is how the move affects the orientation and position of cubies.

Definition 2.1. *We describe the effects of a move, $M \in \mathcal{S}$, with the tuple $(\psi(M), \Theta_M)$, with $\psi(M) \in Aut(C_A), \Theta_M \in (\mathbb{Z}/3\mathbb{Z})^8_\star$.*

These move-representing tuples will be the elements of $\mathcal{R}$, so now we just need a binary operation, and that's where semi-direct product comes in.

To set up a semi-direct product between $Aut(C_A)$ and $(\mathbb{Z}/3\mathbb{Z})^8_\star$ we can use the homomorphism from earlier, f, however we will change codomain to now have $g : Aut(C_A) \to Aut((\mathbb{Z}/3\mathbb{Z})^8_\star)$. We are now ready to define a binary operator, $*_g$.

$$*_g : ((Aut(C_A) \times (\mathbb{Z}/3\mathbb{Z})^8_\star) \times (Aut(C_A) \times (\mathbb{Z}/3\mathbb{Z})^8_\star)) \to (Aut(C_A) \times (\mathbb{Z}/3\mathbb{Z})^8_\star)$$

The function $*_g$ tells us what happens we perform the move sequence MM' with $M, M' \in \mathcal{S}$, $M = \{\rho, \Theta\}, M' = \{\rho', \Theta'\}$ we have

$$\{\rho, \Theta\} *_g \{\rho', \Theta'\} = \{\rho\rho', \Theta' + g(\rho)\Theta\}$$

This is derived from the expressions we got in the previous sections for position and orientation of cubies.

We can now define the a semi-direct product $Aut(C_A) \rtimes_g (\mathbb{Z}/3\mathbb{Z})^8_\star$ as being the group $(Aut(C_A) \times (\mathbb{Z}/3\mathbb{Z})^8_\star, *_g)$. This group is the set of possible orientations and cubie positions obtainable from moves in $\mathcal{S}$, which is what we wanted for $\mathcal{R}$. Hence we define $\mathcal{R}$ as $Aut(C_A) \rtimes_g (\mathbb{Z}/3\mathbb{Z})^8_\star$.

2.3.2 The order of $\mathcal{R}$

Now we have finally defined $\mathcal{R}$ we can find the order of it, from Proposition 1.5 we have that the order of the group $Aut(C_A) \rtimes_g (\mathbb{Z}/3\mathbb{Z})^8_\star$ is equal to the order of $Aut(C_A)$ times the order of $(\mathbb{Z}/3\mathbb{Z})^8_\star$. The order of $(\mathbb{Z}/3\mathbb{Z})^8$ is equal to 3^8 as it is a set of 8 elements, each of which could have 3 values, so the order of $(\mathbb{Z}/3\mathbb{Z})^8_\star$ will be $\frac{3^8}{3}$ as it is the group where the elements can only sum to a multiple of 3. As $Aut(C_A)$ is the same as the symmetric group S_8, we know it must have order 8!. This tells us that $|\mathcal{R}| = 8! \times 3^7$, however, technically the number of possible configurations is much lower. Consider a dice, any of the 6 numbers could be on top, and then that top face could be rotated four times about the vertical axis of symmetry, so we get the total number of ways a cube can be orientated to be 24. This means any configuration of the cube can be orientated in 24 different ways, so whilst $|\mathcal{R}| = 8! \times 3^7$, the number of possible configurations is in fact $\frac{8! \times 3^7}{24} = 3674160$.

3 Properties of a Move Sequence

In this chapter we will explore how long it takes for a move sequence to cycle back to a cube's solved state. We will find the order of elements of $\mathcal{R}$, as this will tell us how many times we need to perform a move until we are performing the identity move (which is the equivalent of the solved cube). Once we have found out how to find the order of a move sequence, we will consider the question 'what is the greatest order of an element of $\mathcal{R}$?'.

3.1 Orders of elements in $\mathcal{R}$

There are two things we need to consider to find the order of an element (ρ, Θ), of $\mathcal{R}$, the order of the permutation $\rho \in C_A$, $|\rho|$ and the order of the orientation $\Theta \in (\mathbb{Z}/3\mathbb{Z})^8_\star$, $|\Theta|$.

The order of the ρ can be found by consider the lengths of the cycles within it. For example, the order of $(c_2, c_3, c_4)(c_6, c_7)$ will be the lowest common multiple, lcm, of the lengths of the individual , so it will be the lcm(3,2) = 6. The order of Θ is considerably easier, as $\Theta \in (\mathbb{Z}/3\mathbb{Z})^8_\star$, so the order of Θ will be the number that when multiplied with each element, θ_i, is 0 mod 3. Therefore for $\theta_i \in \{0, 1, 2\}$, $|\Theta|$ is either 3, or 1 if every θ_i is 0.

Theorem 3.1. *The order of a move, M, represented by $(\psi_M, \Theta_M) \in \mathcal{R}$ is equal to $|\psi_M| \times |\Theta_{M^{|\psi_M|}}|$.*

Proof. If we repeat the move M $|\psi_M|$ times, all the cubies will be back in their original position. However the orientations could be in any state, hence we need to consider how $M^{|\psi_M|}$ changes orientation. We know that $M^{|\psi_M|}$ preserves cubie location, therefore

$$\Theta_{M^{|\psi_M|}} + g\left(\psi_{M^{|\psi_M|}}\right)\Theta_{M^{|\psi(M)|}} = \Theta_{M^{|\psi(M)|}} + \Theta_{M^{|\psi_M|}}$$

Therefore the move $M^{|\psi(M)|}$ needs to be repeated $|\Theta_{M^{|\psi(M)|}}|$ times to correct the cubie orientations to that of the solved state.
Hence $|(\psi(M), \Theta_M)| = |\psi(M)| \times |\Theta_{M^{|\psi(M)|}}|$ □

Remark 3.1. *Finding the orientations is often a tedious task, and so finding $|\Theta_{M^{|\psi(M)|}}|$ will usually take a long time. However, we can modify our orientation formula, $\Theta_{M_1M_2} = \Theta_{M_2} + g(\psi_{M_2})\Theta_{M_1}$, by setting $M_1 = M_2 := M$ to get*

$$\Theta_{M^2} = \Theta_M + g(\psi_M)\Theta_M$$

Which leads to the following lemma.

Lemma 3.2. *For the move sequence $(\psi_M, \Theta_M) \in \mathcal{R}$, $\forall n \in \mathbb{N}$*

$$\Theta_{M^n} = \sum_{i=0}^{n-1}\left[g\left(\psi_M^i\right)\Theta_M\right]$$

Proof. We already have the base case for $n = 1$, as this states $\Theta_{M^1} = \Theta_M$, which is true. Assume it is true for $n = k$, so $\Theta_{M^k} = \sum_{i=0}^{k-1} g\left(\psi_M^i\right)\Theta_M$. For $n = k + 1$, consider

$$\begin{aligned}\Theta_{M^{k+1}} = \Theta_{M^kM} &= \Theta_M + g(\psi_M)\Theta_{M^k}\\ &= \Theta_M + g(\psi_M)\sum_{i=0}^{k-1}\left[g\left(\psi_M^i\right)\Theta_M\right]\\ &= \Theta_M + \sum_{i=1}^{k}\left[g\left(\psi_M^i\right)\Theta_M\right] = \sum_{i=0}^{k}\left[g\left(\psi_M^i\right)\Theta_M\right]\end{aligned}$$

And we are done. □

Example 3.1. *Consider the move FR, i.e. rotating the front face 90° clockwise, then then the right face 90°. To find the order of this move, we need to represent this in the form $(\rho, \Theta_{FR}) \in \mathcal{R}$, and then find the orders of ρ and Θ_{FR}.*

$$\rho = \psi(FR) = \psi(F)\psi(R) = (c_3, c_8, c_5, c_4)(c_2, c_7, c_8, c_3) = (c_2, c_7, c_8, c_5, c_4)$$

Hence $|\rho| = 5$, so now we must find $|\Theta_{(FR)^5}|$.
We can easily find Θ_{FR} as follows;

$$\Theta_{FR} = \Theta_R + g(\rho)\Theta_F = \{0, 1, 2, 1, 2, 0, 1, 2\}$$

And using Lemma 3.2 we get that;

$$\begin{aligned}\Theta_{(FR)^5} &= \sum_{i=0}^{4} \left[g\left(\rho^i\right)\Theta_{FR}\right] \\ &= \{0, 1, 2, 1, 2, 0, 1, 2\} + ... + (\theta_2, \theta_4, \theta_5, \theta_8, \theta_7)\{0, 1, 2, 1, 2, 0, 1, 2\} \\ &= \{0, 1, 1, 1, 1, 0, 1, 1\}\end{aligned}$$

Therefore $|\Theta_{(FR)^5}| = 3$, so we get that $|FR| = |\rho| \times |\Theta| = 5 \times 3 = 15$.

3.2 The Element of Greatest Order

To find the greatest possible order of an element of $\mathcal{R}$ first we will look into the maximum value of $|\rho|$ and $|\Theta|$.
We have seen the greatest value of $|\Theta|$ is 3, but $max(|\rho|)$ is slightly more complex. We must consider all the possible cycle length combinations for C_A. Clearly the possible cycle lengths are 1,2,3,4,5,6,7 and 8, so to find the maximum value of ρ we must find the combination of these with the maximal lowest common multiple. We will ignore the cycles of length 1, as these will not affect the lcm. We denote the number of cycles with a length greater than one in the permutation by $c(\rho)$.

$c(\rho) = 1$ The value of $|\rho|$ will be the longest cycle length, as all other cycles will be of length 1, so in this case $max(|\rho|) = 8$.

$c(\rho) = 2$ Here we have to consider the possible combinations of two of cycle lengths that sum to less than 8, this leaves us with $(2, 3)$, $(2, 4)$, $(2, 5)$, $(2, 6)$, $(3, 4)$, $(4, 4)$ and $(3, 5)$. The maximum lowest common multiple of these is 15 in the case of $(3, 5)$, so $max(|\rho|) = 15$

$c(\rho) = 3$ The only case here could be (2,3,3), and the lcm(2,3,3) = 6.

$c(\rho) = 4$ Here we have (2,2,2,2) which clearly has an lcm of 2.

$c(\rho) \geq 4$ There are no more combinations.

We now have shown that the $max(|\rho|) = 15$ and $max(|\Theta|) = 3$. From this we can get our upper bound for the greatest possible order.

Theorem 3.3. *The upper bound for the order of an element in $\mathcal{R}$ is 45.*

Proof. Consider the move M, for this move to have the greatest order, it would have to be represented by $(\psi(M), \Theta_M)$ where $|\psi(M)| = max(|\rho|) = 15$, and Θ_M will be the $\Theta_M \in \Theta \in (\mathbb{Z}/3\mathbb{Z})^8_\star$ such that $max(|\Theta_{M^{|\psi|)}}|) = 3$.
Hence by Theorem 3.1. we get that the order of this move M will be $15 \times 3 = 45$. □

To show that an element of this order exists, I wrote a simple computer program using C which cycled through the order of Rubik's Cube moves. The program produced the move sequence UFUB, which can be shown to be of order 45 using the methods in Example 3.1, or by cycling through the iterations on the cube. Hence the maximal order of an element of $\mathcal{R}$ is 45.

References

[**1**] A Book of Abstract Algebra. *Charles C. Pinter.* Dover. *Second Edition.*

[**2**] Generators and Fundamental Regions. *Clint McCrory.*
http://www.math.uga.edu/ clint/2005/5210/gens.htm

[**3**] The Symmetry Group of the Triangle. *Arfur Dogfrey.*
http://dogschool.tripod.com/trianglegroup.html

[**4**] On Rubik's Cube. *Olof Bergvall, Elin Hynning, Mikael Hedburg, Joel Mickelin, Patrick Masawe.*
http://www.math.kth.se/ boij/kandexjobbVT11/Material/rubikscube.pdf

[**5**] Group Theory and the Rubiks Cube. *Janet Chen.*
http://www.math.harvard.edu/ jjchen/docs/Group%20Theory%20and%20the%20Rubik's%20Cube.pdf

[**6**] Adventures in Group Theory: Rubiks Cube, Merlins Machine, and Other Mathematical Toys. *David Joyner.*
http://mike.verdone.ca/media/rubiks.pdf

Resources

1. A useful 2-Cube simulator. *Jaap Scherphuis.*
http://home.everestkc.net/ehess/cube2.html

Appendix

The C program which found UFUB can be found at http://pastebin.com/zCx8d4z3 (Warning; INCREDIBLY inefficient, it was made simply to find the move).