Rubik's cube and Group Theory

by

Carl Joakim Isaksen

Thesis

for the degree of

MASTER OF SCIENCE

(Master i Anvendt matematikk og mekanikk)

Faculty of Mathematics and Natural Sciences
University of Oslo

June 2012

Det matematisk- naturvitenskapelige fakultet
Universitetet i Oslo

Acknowledgments

I would like to thank my professor, Geir Ellinsrud, who has been persistent in showing me how he thinks this should be done and yet patient in letting me discover that he was right. He has helped much with the proofs of Lemmas 3.1.10 and 3.1.11. I would like to thank my wife, Marianne Isaksen, who has taken care of our kids so I could be given the time needed to finish this thesis and Krisitan Rannestad who has also given me some much needed guidance in defining the right group. I would also like to thank my brother, Stefan Isaksen, who taught me how to solve the cube when I was younger. His method is has been slightly improved and is described in chapter 6.

Contents

Chapter 1

Introduction

The more you study mathematics the more you try to define what mathematics really is. That is how it is for me anyways. In light of this question I typed "math" in wikipedia to see what sort of definition it would give me. I soon forgot why I was looking up "math" and focused my attention on an overview of some of the main fields in mathematics. There was a picture connected to each field. Calculus had the area under a curve, topology had a 3D model of a torus and so on. Then I saw something interesting. The picture next to "group theory" was a Rubik's cube. I've known how to solve the cube since I was in my early teens and I had just finished a course in group theory which I really enjoyed. Could the two be added together? It was almost too good to be true.
I was given the following research topic to base my thesis on:

Research topic: The thesis is centered on the Rubic's cube and the group it defines. Give a description of the group structure by using groups of permutation and the orientation groups of the corner and side cubits. Describe interesting subgroups, e.g. the center and subgroups of elements which only changes orientation. Describe, by use of group theory, simple moves e.g. moves which only changes orientation of two corners. Give an overview of some algorithms which solves the cube.

I start by creating the group in chapter 2 as a quotient group of a group on six letters. I will show that this group has the desired properties the Rubik's group should have. Chapters 3 and 4 are devoted to understand the possibilities and limitations of the group which will result in a complete mapping of the group as a semidirect product. The theory in chapter 3 has been sketched out by Michael Weiss [6] and I have expanded upon it. In the short chapter 5 I will determine the center of the group. I will present a method for solving the cube in chapter 6.

Notation

- Since there will be both vectors and cycles in this thesis I will use $(a_1, a_2, \dots, a_n)$ for vectors with n coordinates and $[a_1, a_2, \dots, a_n]$ for a cycle that sends a_1 to a_2 etc.
- $\mathbb{Z}/(n)\mathbb{Z} = \mathbb{Z}_n$.
- If a proof is omitted (either because it is trivial or similar to a previous proof) I will simply put

  Proof. □
- For a homomorphism $\phi : G_1 \to G_2$ the kernel of ϕ is defined as

$$\ker(\phi) = \{g \in G_1 \mid \phi(g) = id_{G_2}\}$$

- A variable $\mathbf{x} = (x_1, \dots, x_n)$ is a vector if it is in bold font.
- $(G, *)$ is the group G with binary relation $*$.

Chapter 2

The group structure of the cube.

2.1 A group on 6 letters

Let $G_6 = \{D, U, B, F, L, R\}$ be a set of six letters and let $g^4 = \emptyset \ \forall \ g \in G_6$, where the $\emptyset$ denotes the empty word. Let G be the set of any finite words of these letters, remembering the relation above.

Definition 2.1.1. *Let* $* : G \times G \to G$ *be the map defined by*

$$*(w_1, w_2) = w_1 * w_2 = w_1 w_2$$

So $*$ *denotes the combination of two such words into a new word.*

Example 2.1.2. $FDBR * R^2DU = FDBR^3DU$

Lemma 2.1.3. $(G, *)$ *is a group. Where* $1 = id_G = \emptyset$

Proof. (i) The right identity comes from the definition. Let $w \in G$, then $w * id_G = w\emptyset = w$
(ii) Since any word is made up of letters from G_6 inverses exists. Take e.g. DUR. Then

$$DUR * R^3U^3D^3 = id_G$$

so for any $g \in G_6$, $g^{-1} = g^3$, and for any word $abc \in G, (abc)^{-1} = c^3b^3a^3 = c^{-1}b^{-1}a^{-1}$.
(ii) This group is closed under $*$ since any two finite words form a new finite word.
(iv) Associativity is trivial since $a(bc) = abc$ and $(ab)c = abc$ hence $a(bc) = (ab)c$ □

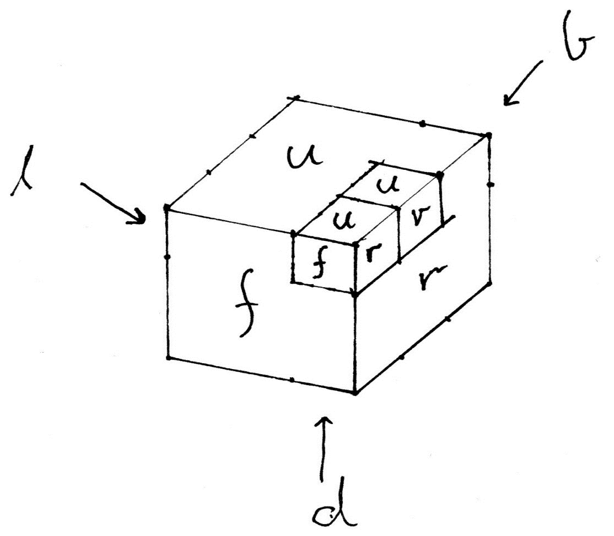


Figure 2.1: The name of the faces and the cubits

2.2 Organizing the cube

The cube has 6 faces. Front (f), back (b), left (l), right (r), top (up (u)) and bottom (down (d)). See figure 2.1. They form a set

$$F = \{f, b, l, r, u, d\}$$

The cube consists of 26 little cubes, hereby known as *cubits*. There are 8 corner cubits with three faces. They will form the set

$$U(C_c) \subset F^3$$

and will have names like $(f, u, r) \in U(C_c)$ or just fur for short, meaning the cubit in the 'front, up, right' position. There 12 side cubits with two faces forming the set

$$U(C_s) \subset F^2$$

with names like $(u, r) \in U(C_s)$ or just ur for short, meaning the cubit in the 'up, right' position. There are also 6 center cubits with only one face, and they will not be studied now for reasons stated later.

Let D be a clockwise 90 degree rotation of the down face when looking right at it. Same for U, B, F, L, R for up, back, front, left and right faces respectively. These 6 basic moves form the set

$$G_6 = \{D, U, F, B, L, R\}$$

The words of the group G can be viewed as moves on the cube where the letters in G_6 are the basic moves. Note that a word from G will only move corner cubits to corner cubits and side cubits to side cubits. The M_F move is moving the middle row vertically 90° through F, U, B, D faces. It is rotated the same way as R, not as L. Note that $M_F = R^{-1}L$, so there is no need to include the words that moves the middle rows and columns as generators. Thus the center cubits will never be moved, making them uninteresting to study. One can formally say that

$$g : F^3 \to F^3$$

$\forall\ g \in G$ with the corner cubits and

$$g : F^2 \to F^2$$

$\forall\ g \in G$ with the side cubits. Starting down this path of extreme formality will only lead to confusion (especially for me) so I chose just to state the following: When I write

$$D(frd) = rbd$$

I mean to say: $f \to r, r \to b, d \to d$. Allow me to remark what this notation gives and what it does not give. It simply says that if any corner cubit is in the frd position and the word D is applied to it then it will end up in the rbd position. It also gives me which face of the different cubits were moved. The front face in frd went to the right face in rbd and so on. It does not state which cubit was in the frd position to start with.

Each cubit will reside in a placeholder which will be called a *cubicle* and will be named in the same fashion as the cubits. They do not move when a word is applied to the cubits. The three letters denoting a corner cubit will always be the same three letters of the cubicle it resides, but they may not be in the same order.

We let B_c be the set of all corner cubicles, they will be defined to be:

$$B_c = \{fur, frd, fdl, flu, bul, bld, bdr, bru\}$$

If you have a cube, you can check that all the individual corner cubicles have been defined clockwise. We let B_s be the set of all side cubicles defined to be:

$$B_s = \{fu, fr, fd, fl, bl, bd, br, bu, ur, ul, dl, dr\}$$

There are three ways a corner cubit may reside in a corner cubicle and two ways a side cubit may reside in a side cubicle. If we look at all possibilities we form the set

$$C_c = \{\text{All possible corner cubit positions}\}$$

so $|C_c| = 8\cdot 3 = 24$. We call this set the *oriented* corner cubits. Compare with $|U(C_c)| = 8$, which is then the set defined earlier, now called the unoriented corner cubits The same can be done with the side cubits forming the set

$$C_s = \{\text{All possible side cubit positions}\}$$

so $|C_s| = 12 \cdot 2 = 24$, and call this the *oriented* side cubits. The sets $B_c = U(C_c)$ and $B_s = U(C_s)$, but the group will act on $U(C_i)$ but not on B_i. If one only needs to speak of oriented or unoriented cubits in general we form the sets:

$$C = C_s \cup C_c$$

being the oriented cubits and

$$U(C) = U(C_c) \cup U(C_s)$$

being the unoriented cubits.

Definition 2.2.1. *Let $\pi_c : C_c \to C_c$ where $abc \in F^3$ are the three letters in the corner cubicle and $\pi_s : C_s \to C_s$ where $ab \in F^2$ are the two letters in the side cubicle, be given by*

$$\pi_c(abc) = \pi_c(bca) = \pi_c(cab) = abc$$

and

$$\pi_s(ab) = \pi_s(ba) = ab$$

π_c and π_s removes the orientation of the cubits, and $\mathrm{Im}(\pi_i) = U(C_i)$. To help us understand how the basic moves move the cubits we make a vector and number it according to the place of the cubits in the cube's solved state. We number the cubits in the order of the cubicles.The corner cubits then form a vector $\mathbf{c} \in C_c^8$. So if the cube is in its start configuration then

$$\mathbf{c} = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$$

When a word from G is applied to $\mathbf{c}$ the order will change. The same ordeal can be done with a $\mathbf{d} \in C_s^{12}$ for the side cubits in a similar fashion. We will let $x_i = \pi_c(c_i)$ and $y_i = \pi_s(d_i)$. Let

$$\mathbf{x} = (\pi_c(c_1), \ldots, \pi_c(c_8)) = (x_1, \ldots, x_8)$$

$$\mathbf{y} = (\pi_s(c_1), \ldots, \pi_s(c_{12})) = (y_1, \ldots, y_{12})$$

How the basic moves act on $\mathbf{x}$ and $\mathbf{y}$ is depicted in table 2.1.

Move	Coordinates
$D(\mathbf{x})$	$(x_1, x_3, x_6, x_4, x_5, x_7, x_2, x_8)$
$D(\mathbf{y})$	$(y_1, y_2, y_{11}, y_4, y_5, y_{12}, y_7, y_8, y_9, y_{10}, y_6, y_3)$
$U(\mathbf{x})$	$(x_4, x_2, x_3, x_5, x_8, x_6, x_7, x_1)$
$U(\mathbf{y})$	$(y_9, y_2, y_3, y_4, y_5, y_6 y_7, y_{10}, y_8, y_1, y_{11}, y_{12})$
$F(\mathbf{x})$	$(x_4, x_1, x_2, x_3, x_5, x_6, x_7, x_8)$
$F(\mathbf{y})$	$(y_4, y_1, y_2, y_3, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12})$
$B(\mathbf{x})$	$(x_1, x_2, x_3, x_4, x_8, x_5, x_6, x_7)$
$B(\mathbf{y})$	$(y_1, y_2, y_3, y_4, y_8, y_5, y_6, y_7, y_9, y_{10}, y_{11}, y_{12})$
$L(\mathbf{x})$	$(x_1, x_2, x_4, x_5, x_6, x_3, x_7, x_8)$
$L(\mathbf{y})$	$(y_1, y_2, y_3, y_{10}, y_{11}, y_6, y_7, y_8, y_9, y_5, y_4, y_{12})$
$R(\mathbf{x})$	$(x_2, x_7, x_3, x_4, x_5, x_6, x_8, x_1)$
$R(\mathbf{y})$	$(y_1, y_9, y_3, y_4, y_5, y_6, y_{12}, y_8, y_7, y_{10}, y_{11}, y_2)$

Table 2.1:

2.3 Group actions

Definition 2.3.1. *Let X be a set and $(G, *)$ be a group. We say that G acts on X (from left) if $\exists$ a map $\circ : G \times X \to X$ such that*
(i) $id_G x = x$
(i) $(g_1 * g_2) \circ (x) = g_1 \circ (g_2 \circ x) \quad \forall\ x \in X \quad$ and $\quad \forall\ g_1, g_2 \in G$

Now, there is a map for each $c \in C$

$$\circ : G \times C \to C$$

so that $w \circ c = w(c)$ simply denotes in which cubicle c is after applying the word w.

Example 2.3.2. $R(fr) = ur$ and $UR(fr) = U(R(fr)) = U(ur) = ub$

It will be important to remember that UR means first do R then do U since G acts from the left.

Lemma 2.3.3. *G acts on C*

Proof. We use the map above.
(i) $1 \circ c = c, \ \forall\ c \in C$
(ii) Let $w_1, w_2 \in G$ and $c \in C$ then

$$(w_1 * w_2) \circ (c) = w_1 \circ (w_2 \circ c)$$

$\forall\ c \in C$ and $\forall\ w_1, w_2 \in G$ from the example above. This should amount to no loss of generality. □

Lemma 2.3.4. *G acts on $\pi_c(C_c) \cong U(C_c)$ and $\pi_s(C_s) \cong U(C_s)$ by the maps*

$$g(\pi_c(c)) = \pi_c(g(c))$$

and

$$g(\pi_s(c)) = \pi_s(g(c))$$

Proof. We will only prove the first, the second is identical.

$$\text{(i)} \quad 1 \circ \pi(c) = \pi(1(c)) = \pi(c), \ \forall \ c \in C$$

(ii) Let $g, h \in G$ and $c \in C$ then

$$(gh)\pi(c) = \pi(gh(c)) = \pi(g(h(c))) = g(\pi(h(c))) = g(h(\pi(c)))$$

$\forall \ c \in C$ and $\forall \ g, h \in G$. □

In simpler language, G acts on both the oriented and unoriented cubes.

2.4 Making the right group

Lemma 2.4.1. *The set*

$$N = \{g \in G \mid g(c) = c \ \forall \ c \in C\}$$

is a normal subgroup of G.

Proof. (i) (subgroup): If $n_1, n_2 \in N$ we have $\forall \ c \in C$

$$(n_1 n_2)(c) = n_1(n_2(c)) = n_1(c) = c \ \Rightarrow n_1 n_2 \in N,$$

$id_G = id_N$, and since $n^{-1}(n(c)) = n^{-1}(c)$ and $n^{-1}(n(c)) = (n^{-1}n)(c) = c$ then $n^{-1} \in N$.
(ii) (normal): Let $g \in G$. Then

$$gng^{-1}(c) = g(n(g^{-1}(c))) = g(g^{-1}(c)) = (gg^{-1})(c) = c$$

so $gng^{-1} \in N \ \forall \ g \in G$ and $n \in N$. □

Definition 2.4.2. *Let $g_1, g_2 \in G$. We say*

$$g_1 \sim g_2$$

if $g_1(c) = g_2(c) \ \forall \ c \in C$.

Lemma 2.4.3. $\sim$ *is an equivalence class.*

Proof. There are three things to check.
(i) Reflexivity: This is trivial since $g(c) = g(c)\ \forall\ g \in G$.
(ii) Symmetry: If $g_1(c) = g_2(c)$ then $g_2(c) = g_1(c)$.
(iii) Transitivity: If $g_1(c) = g_2(c)$ and $g_2(c) = g_3(c)$ then $g_1(c) = g_3(c)$. □

Lemma 2.4.4. *The following is equivalent:*
(i) $\exists\ g \in N$ *such that* $g_1 = gg_2$
(ii) $g_1 g_2^{-1} \in N$
(iii) $g_1 \sim g_2$

Proof. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i). Suppose $\exists\ g \in N$ such that $g_1 = gg_2$. Then

$$(g_1 g_2^{-1})(c) = (g g_2 g_2^{-1})(c) = g(c) = c$$

so $g_1 g_2^{-1} \in N$. Now suppose $g_1 g_2^{-1} \in N$ then

$$(g_1 g_2^{-1})(c) = c \iff g_1(c) = g_2(c)$$

hence $g_1 \sim g_2$. And if $g_1 \sim g_2$ then for any $g \in N$ we have:

$$g_1(c) = g_2(c) \iff g_1(c) = g(g_2(c)) \iff g_1(c) = (gg_2)(c)$$

□

Proposition 2.4.5.

$$\mathbb{G} = G/N$$

is a finite group. The elements in this group will be called moves.

Before this is proven, let me note that $\mathbb{G}$ will be the group studied in the rest of this thesis. It will have the desired properties the group of the Rubik's cube should have. The lemma above tells us that two different words that gives the same configuration on the cube will be one move in $\mathbb{G}$. We will also use $m \in \mathbb{G}$ for a general move and $g \in G_6$ for one of the six basic moves in the rest of the thesis.

Proof. Since N is normal, $\mathbb{G}$ is a group. So the interesting point here is the finiteness. Since two different paths to the same configuration is now one move all one has to consider is the number of possible configurations of the cube. There are 8 corners with 3 orientations each and 12 sides with 2. As noted earlier, the center cubits do not move relative to each other. So there is a maximum of $8! \cdot 3^8 \cdot 12! \cdot 2^{12} \approx 5,2 \cdot 10^{20}$ different configurations on the cube, which is a finite number (almost not...). □

So $|\mathbb{G}| \leq 8! \cdot 3^8 \cdot 12! \cdot 2^{12}$. Since $\mathbb{G}$ is a quotient group, which move should represent a co-set? In $\mathbb{Z}/(3)\mathbb{Z}$ -1,0 or 1 are natural selections but what about $\mathbb{G}$? Since a move may be almost infinitely long, a logical answer would be the shortest one. There are, in fact, an upper limit to the length of any move. It has been proven that the cube can come from any configuration to the start configuration in 20 or less moves (letters), which will not be proven in this thesis. This gives us that any $m \in \mathbb{G}$ need not be longer than 20 letters. [1]

Corollary 2.4.6. $\langle G_6 \rangle = \mathbb{G}$

Proof. This follows strait from how $\mathbb{G}$ has been defined. One needs to confirm that non of the basic moves are in N which is obvious. □

We have the following:

Corollary 2.4.7.

$$\{1\} \to N \to G \to \mathbb{G} \to \{1\}$$

is an exact sequence.

Proof. □

2.5 Introducing ϕ

Definition 2.5.1. *Let X be a set. A* permutation *of X is a function $\sigma : X \to X$ which is bijective.*

Theorem 2.5.2. *Let G be a group which acts on X. For each $g \in G$, the function $\sigma_g : X \to X$ defined by*

$$\sigma_g(x) = gx$$

$\forall\ x \in X$ is a permutation of X.

Proof. See page 155 in [1] □

Proposition 2.5.3. *Let X be a set with $n \in \mathbb{N}$ elements and σ be a permutation of X. Then*

$$S_n = \{\sigma : X \to X\}$$

is a group under function composition ($\circ$) with $n!$ elements called the symmetry group of n letters.

Proof. See page 77 in [1] □

[1] See appendix A

If we forget about the orientation of the cubits we see that $\mathbb{G} \cong \Omega \subset (S_8 \times S_{12})$ since $\mathbb{G}$ permutes all the corner and side cubits. If one numbered all the unoriented corner and side cubits in any fashion a natural map would arise:

$$\phi : \mathbb{G} \to (S_8 \times S_{12})$$

where $\phi(m) = \sigma_m$ for a $\sigma \in (S_8 \times S_{12})$. Since corners only go to corners and sides to sides one could divide the map into this:

$$\phi_c : \mathbb{G} \to S_8 \text{ given by } \phi([x_i, \ldots, x_j]) = [i, \ldots, j] \text{ where } x_i \in U(C_c)\ \forall\ i \in \mathbb{N}$$
$$\phi_c : \mathbb{G} \to S_{12} \text{ given by } \phi([y_l, \ldots, y_k]) = [l, \ldots, k] \text{ where } y_i \in U(C_s)\ \forall\ i \in \mathbb{N}$$

So $\mathrm{Im}(\phi) = \Omega \subset (S_8 \times S_{12})$. The $\ker \phi$ would be all the moves that only changes orientation of the cube. Let's call it $\mathbb{H}$. This would give rise to the following exact sequence:

$$\{1\} \to \mathbb{H} \to \mathbb{G} \to \Omega \tag{2.1}$$

The next two chapter will be devoted to determine $\mathbb{H}$ and Ω. They will play an important role in understanding $\mathbb{G}$.

Chapter 3

$\mathbb{H}$ and orientation

What is the subgroup $\mathbb{H}$ from (2.1)? $\mathbb{H}$ consits of moves which does not permute any cubits but simply changes their orientation.

Lemma 3.0.4. *$\mathbb{H}$ is a normal subgroup.*

Proof. Since $\mathbb{H} = \ker(\phi)$. □

Since corner cubits cannot go to side cubits and visa versa, we will analyze them separately.

3.1 Corner cubits

We will start by looking at the corner cubits. Much of this section has been done by Michael Weiss [6], in what my professor called "perhaps the simplest, non-trivial example of gauge theory". (You do not need to know any gauge theory to understand this). We can say that the cubits are twisted and give them value. 0 for no twist, 1 for a clockwise twist and -1 for a counterclockwise twist, and try to define

$$\tau(m, c) = \text{The amount } c \text{ is twisted by } m \in \mathbb{G}$$

One problem is that the basic moves also move the cubits from cubicle to cubicle so "measuring" the twists may be tricky. This twist function will have certain interesting and very helpful properties. In the end we shall be able to prove the following:

Theorem 3.1.1. *If the cube is in its start configuration then*

$$\sum_{c \in C_c} \tau(m, c) \equiv 0 \mod 3$$

$\forall\, m \in \mathbb{G}$

The first problem will be to properly define a twist.

Definition 3.1.2. *A* fiber *over a* $x \in U(C_c)$ *is*

$$\pi^{-1}(x)$$

(π from definition 2.2.1)

Hence, the fiber is the three ways a cubit can sit in a cubicle. ($|\pi^{-1}(x)| = 3$). Now 'flu' can be in the 'flu' cubicle in three ways: 'flu', 'luf' or 'ufl'. A close look shows that 'flu' is permuted cyclically. We will call the group that permutes the $c \in C_c$ in its own fiber Z_3. The choice of fiber is trivial since they each have 3 elements.

Lemma 3.1.3.

$$Z_3 \cong \mathbb{Z}_3$$

Proof. Define $\gamma_i \in Z_3,\ \gamma_i : C_c \to C_c$ by

$$\begin{aligned}\gamma_0(abc) &= abc\\ \gamma_1(abc) &= cba\\ \gamma_{-1}(abc) &= bca\end{aligned}$$

Then $\lambda : Z_3 \to \mathbb{Z}_3$ given by

$$\lambda(\gamma_i) = i$$

is an isomorphism. □

So we let $\mathbb{Z}_3$ act from the right while $\mathbb{G}$ acts from the left.

Lemma 3.1.4. *For* $m \in \mathbb{G}, c \in C_c$ *and* $t \in \mathbb{Z}_3$ *we have*

$$(mc)t = m(ct)$$

Proof. Let $m(c_i) = c_j + 1$. Let $(c_i)t = c_i + 1\ \forall\ c \in C_c$. Then $(mc_i)t = (c_j + 1)t = c_j + 2 = c_j - 1$, and $m(c_it) = m(c_i + 1) = c_j + 2 = c_j - 1$. □

Lemma 3.1.5. $\mathbb{Z}_3$ *acts transitively on each fiber of* C_c.

Proof. This is only an observation on how the cube works. If a cubit is in a certain orientation then there exists a move such that the cubit can be rotated in any way we want. □

Lemma 3.1.6. $\mathbb{G}$ *acts transitively on* $U(C_c)$

Proof. This is another observation on how the cube works. If a corner cubit is in a certain cubicle then there exists a move such that the cubit can be moved to any other corner cubicle. □

The twist can now be defined as follows:

Definition 3.1.7. *If c and mc are in the same fiber then we say that $mc = ct$ for a unique $t \in \mathbb{Z}_3$ and define*

$$\tau(m, c) = t$$

What if c and mc are not in the same fiber? It seems that some kind of coordinate system would be useful, but it could turn out to be very messy. Another option is to use *sections*, which is quite frequent in gauge theory.

Definition 3.1.8. *A* section *of C_c is a set S that picks one element from each fiber.*

So, if S is a section and $x \in U(C_c)$ then

$$S(x) = \text{the chosen element of the fiber over } x$$

So

$$S(x) \in \pi^{-1}(x)$$

Let $S(x) \in C_c$ then $\pi(S(x))) = x$. Let m be a move that sends x to another fiber. Let m^{-1} send x to $m^{-1}x$ and then back to C_c by $S(m^{-1}x)$. Finally send this back to the start fiber by m:

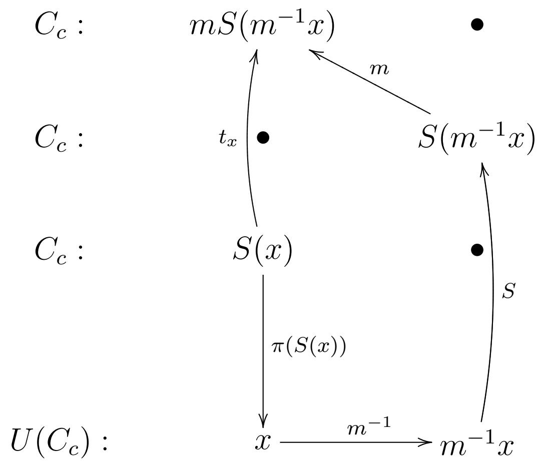
$$mS(m^{-1}x)$$

Now, $mS(m^{-1}x)$ is in the same fiber as $S(x)$ $\forall\ m \in \mathbb{G}$ but not necessarily in the same orientation. We can now define a more general twist function.

Definition 3.1.9.

$$\tau(m, S, x) = \textit{the unique } t_x \in \mathbb{Z}_3 \textit{ such that } S(x)t_x = mS(m^{-1}x)$$

(note that this is possible because $\mathbb{Z}_3$ acts transitively on the fibers, and because $\mathbb{G}$ acts transitively on the unoriented cubits). This whole ordeal is depicted in the following diagram where the black dots represent unused cubits in the fiber, the equation comes if you start at $S(x)$.



What if we had chosen another section? Since $\mathbb{Z}_3$ cyclically permutes elements in the fibers, we see that a section R will have the following relation to section S:

$$R\mathbf{z} = S$$

for a $\mathbf{z} \in \mathbb{Z}_3^8$ and

$$R(x)z_x = S(x)$$

for some $z_x \in \mathbb{Z}_3$, which will be the $x'th$ coordinate of $\mathbf{z} \in \mathbb{Z}_3^8$. We can prove the following:

Lemma 3.1.10. *If S and R are any two sections of C_c then*

$$\sum_{x \in U(C_c)} \tau(m, S, x) = \sum_{x \in U(C_c)} \tau(m, R, x)$$

Proof.

$$\begin{aligned} R(x)z_x &= S(x) \\ \Rightarrow R(m^{-1}x)z_{m^{-1}x} &= S(m^{-1}x) \text{ now let m act} \\ \Rightarrow mR(m^{-1}x)z_{m^{-1}x} &= mS(m^{-1}x) \\ \Rightarrow R(x)\tau(m, R, x)z_{m^{-1}x} &= S(x)\tau(m, S, x) \text{ from 3.1.9} \\ \Rightarrow R(x)\tau(m, R, x)z_{m^{-1}x} &= R(x)z_x\tau(m, S, x) \text{ additively:} \\ \Rightarrow \tau(m, R, x) + z_{m^{-1}x} &= z_x + \tau(m, S, x) \end{aligned}$$

Summing over:

$$\sum_{x \in U(C_c)} \tau(m, R, x) + \sum_{x \in U(C_c)} z_{m^{-1}x} = \sum_{x \in U(C_c)} z_x + \sum_{x \in U(C_c)} \tau(m, S, x)$$

$$\sum_{x \in U(C_c)} \tau(m, R, x) = \sum_{x \in U(C_c)} \tau(m, S, x)$$

so the sum is only dependent on m, not on the section. $\square$

The next lemma will be particularly usefull.

Lemma 3.1.11. *$\zeta : \mathbb{Z}_3^8 \to \mathbb{Z}_3$ given by*

$$\zeta(\tau(m, S, \mathbf{x})) = \sum_{x_i \in U(C_c)} \tau(m, S, x_i)$$

where each x_i is a coordinate of $\mathbf{x}$, is a homomorphism*.*

Proof. Let $m, h \in \mathbb{G}$. Remember that

$$S(x)\tau(h, S, x) = hS(h^{-1}x)$$

We have

$$\begin{aligned} S(x)\tau(m, S, x) &= ms(m^{-1}x) \\ \Rightarrow S(x)\tau(hm, S, x) &= hmS(m^{-1}h^{-1}x) \end{aligned}$$

also

$$S(h^{-1}x)\tau(m, S, h^{-1}x) = mS(m^{-1}h^{-1}x)$$

Now letting h act from the right and using the other identities gives:

$$\begin{aligned} hS(h^{-1}x)\tau(m, S, h^{-1}x) &= hmS(m^{-1}h^{-1}x) \\ \Rightarrow S(x)\tau(h, S, x)\tau(m, S, h^{-1}x) &= S(x)\tau(hm, S, x) \\ \Rightarrow \tau(h, S, x)\tau(m, S, h^{-1}x) &= \tau(hm, S, x) \end{aligned}$$

Additively this gives:

$$\tau(h, S, x) + \tau(m, S, h^{-1}x) = \tau(hm, S, x) \tag{3.1}$$

$$\begin{aligned} \Rightarrow \sum_{x \in U(C_c)} \tau(h, S, x) + \sum_{x \in U(C_c)} \tau(m, S, x) &= \sum_{x \in U(C_c)} \tau(hm, S, x) \\ \Rightarrow \zeta(\tau(h, S, x)) + \zeta(\tau(m, S, x)) &= \zeta(\tau(hm, S, x)) \end{aligned}$$

we've replaced $h^{-1}x$ with x when the sum comes since all the unoriented cubits will be summed over. $\square$

This gives us the desired results and a corollary which will be important later on.

Corollary 3.1.12. *Let $m, n \in \mathbb{G}$ and τ be as before. Then*

$$\tau(mn, S, x) = \tau(m, S, x) + \tau(n, S, m^{-1}x)$$

Proof. This is equation (3.1). □

This also holds for the side cubits as we shall see later on.

Definition 3.1.13. *S is a section such that*

$$\tau(1, S, \mathbf{x}) = 0$$

and

$$\tau(1, S, \mathbf{y}) = 0$$

when the cube is in its start configuration.

To see that the sum is always zero, we need to see what happens with the six basic moves under S . If S is the cubicles then it satisfies definition 3.1.13 and we give value 1 for clockwise twist and -1 for counterclockwise twist.

Example 3.1.14. *We see that $D(x_2) = x_7$ and $D(frd) = rbd$ while the cubicle is bdr. So*

$$S(x_7)\tau(D, S, x_7) = DS(D^{-1}x_7) = DS(x_2) = D(frd) = rbd$$

$$\Rightarrow bdr + \tau(D, S, x_7) = rbd$$

$$\Rightarrow \tau(D, S, x_7) = 1$$

In other words, we need to twist x_7 clockwise from its cubicle state in order to achieve the same twist as D gives it when it comes from the cubicle state of x_2.

Continuing like this gives us table 3.1. We can now finally prove the following

Theorem 3.1.15. *If R is a section such that $\zeta(\tau(1, R, x)) = 0$ then*

$$\zeta(\tau(m, R, x)) \equiv 0 \mod 3$$

for all $m \in \mathbb{G}$. In particular

$$\zeta(\tau(m, S, x)) \equiv 0 \mod 3$$

Move	Coordinates
$\tau(D, S, \mathbf{x})$	(0,-1,-1,0,0,-1,1,0)
$\tau(D, S, \mathbf{y})$	(0,0,1,0,0,1,0,0,0,0,1,1)
$\tau(U, S, \mathbf{x})$	(1,0,0,-1,1,0,0,-1)
$\tau(U, S, \mathbf{y})$	(1,0,0,0,0,0,0,1,1,1,0,0)
$\tau(F, S, \mathbf{x})$	(0,0,0,0,0,0,0,0)
$\tau(F, S, \mathbf{y})$	(0,0,0,0,0,0,0,0,0,0,0,0)
$\tau(B, S, \mathbf{x})$	(0,0,0,0,0,0,0,0)
$\tau(B, S, \mathbf{y})$	(0,0,0,0,0,0,0,0,0,0,0,0)
$\tau(L, S, \mathbf{x})$	(0,0,-1,1,-1,1,0,0)
$\tau(L, S, \mathbf{y})$	(0,0,0,0,0,0,0,0,0,0,0,0)
$\tau(R, S, \mathbf{x})$	(-1,1,0,0,0,0,-1,1)
$\tau(R, S, \mathbf{y})$	(0,0,0,0,0,0,0,0,0,0,0,0)

Table 3.1:

Proof. Lemma 3.1.10 gives us that we can just use S. We see that $\zeta(\tau(1, S, x)) = 0$ when the cube is solved. From table 3.1 we see that

$$\zeta(\tau(g, S, x)) \equiv 0 \mod 3$$

$\forall\ g \in G_6$. Now each $m \in \mathbb{G}$ can be written as $m = \prod g_i$, where $g_i \in G_6\ \forall\ i$. The homomorphism property then gives:

$$\zeta(\tau(m, S, x)) = \zeta(\tau(\prod g_i, S, x)) = \sum_i \zeta(\tau(g_i, S, x)) \equiv 0 \mod 3$$

□

3.2 Side cubits

Now a similar law holds for side cubits modulo 2. This section will be very similar to the last, if the proofs are similar I will just state

Proof. □

Here the cubits are twisted with value 0 for no twist and 1 for a twist. The fiber now only has two elements and we will use $y \in U(C_s)$.

Definition 3.2.1. *A* fiber *over a $y \in U(C_s)$ is*

$$\pi^{-1}(y)$$

Lemma 3.2.2.

$$S_2 \cong \mathbb{Z}_2$$

Proof. □

So we let $\mathbb{Z}_2$ act on the right.

Lemma 3.2.3. *For $m \in \mathbb{G}$, $c \in C_s$ and $t \in \mathbb{Z}_3$ we have*

$$(mc)t = m(ct)$$

Proof. The only difference is that -1 is no longer an option. □

The twist can now be defined as:

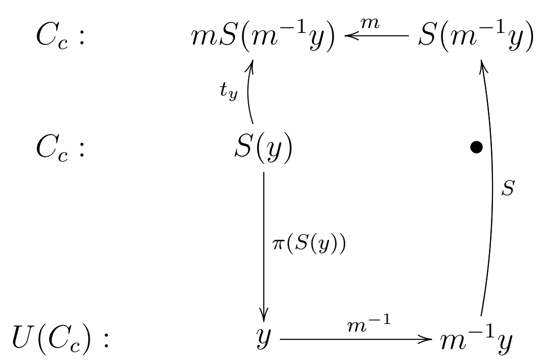
Definition 3.2.4. *If c and mc are in the same fiber then we say that $mc = ct$ for a unique $t \in \mathbb{Z}_2$ and define*

$$\tau(m, c) = t$$

$\mathbb{Z}_2$ acts transitively on the fibers of C_s as well, $\mathbb{G}$ acts transitively on $U(C_s)$ and a section Q is the same, only with 12 elements. We have the same important relation:

Definition 3.2.5.

$$\tau(m, Q, y) = \textit{the unique } t_y \in \mathbb{Z}_3 \textit{ such that } Q(y)t_y = mQ(m^{-1}y)$$



The independence of sections when taking sums follow from the same calculations, ending up with:

$$\sum_{y \in U(C_s)} \tau(m, R, y) = \sum_{y \in U(C_s)} \tau(m, Q, y)$$

The homomorphism property holds

Lemma 3.2.6. *$\zeta : \mathbb{Z}_2^{12} \to \mathbb{Z}_2$ given by*

$$\zeta(\tau(m, Q, \mathbf{y})) = \sum_{y \in U(C_s)} \tau(m, Q, y)$$

is a homomorphism.

Proof. □

Corollary 3.1.12 also holds with y instead of x. We use the section S from definition 3.1.13 and we can now prove the analogue for side cubits.

Theorem 3.2.7. *If Q is a section such that $\zeta(\tau(1, Q, y)) = 0$ then*

$$\zeta(\tau(m, Q, y)) \equiv 0 \mod 2$$

for all $m \in \mathbb{G}$. In particular

$$\zeta(\tau(m, S, y)) \equiv 0 \mod 2$$

Proof. We can again just use S. We see that $\zeta(\tau(1, S, y)) = 0$ when the cube is solved. From table 2 we see that

$$\zeta(\tau(g, S, y)) \equiv 0 \mod 2$$

$\forall\ g \in G_6$. Now each $m \in \mathbb{G}$ can be written as $m = \prod g_i$, where $g_i \in G_6\ \forall\ i$. The homomorphism property then gives:

$$\zeta(\tau(m, S, y)) = \zeta(\tau(\prod g_i, S, y)) = \sum_i \zeta(\tau(g_i, S, y)) \equiv 0 \mod 2$$

□

3.3 Back to $\mathbb{H}$

Lemma 3.3.1. *$\tau : (\mathbb{H}, C, U(C)) \to (\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12})$ as defined earlier is a homomorphism.*

Proof. Let $h_1, h_2 \in \mathbb{H}$. Corollary 3.1.12 gives us that

$$\tau(h_1 h_2, S, x) = \tau(h_1, S, x) + \tau(h_2, S, h_1^{-1} x)$$

but $h_1^{-1} x = x$ since $h_1 \in \mathbb{H}$ and $\mathbb{H}$ is a group. Same argument shows that it holds for y as well. □

So what about $\mathbb{H}$? From what has been done it would be plausible to conclude that

$$\mathbb{H} \cong K \subset (\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12})$$

Where

$$K = \{(\mathbf{x}, \mathbf{y}) \in (\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}) \mid \zeta(\tau(g, s, x)) \equiv 0 \mod 3,\ \zeta(\tau(g, s, y)) = 0 \mod 2\, \forall g \in \mathbb{G}\}$$

And since the sums have to be equal we see that

$$K \cong (\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11})$$

$\mathbb{H} \cong K$ is only true if the homomorphism from $\mathbb{H}$ to K is surjective. There might be some $\mathbf{a} = (a_1, \ldots, a_8) \in \mathbb{Z}_3^8$ where

$$\sum_i a_i \equiv 0 \mod 3$$

but there would be none $h \in \mathbb{H}$ such that

$$\tau(h, S, \mathbf{x}) = \mathbf{a}$$

We must prove the following.

Theorem 3.3.2. *Let $m \in \mathbb{G}$. Then $m \in \mathbb{H}$ if and only if*

$$\zeta(\tau(m, S, x)) \equiv 0 \mod 3$$

$\forall\ x \in U(C_c)$ and

$$\zeta(\tau(m, S, y)) \equiv 0 \mod 2$$

$\forall\ y \in U(C_s)$.

Before this can be proven we will have need of the following two lemmas:

Lemma 3.3.3. *Let $x_i, x_j, x_i', x_j' \in U(C_c)$, where $x_i \neq x_j \neq x_j'$. Then $\exists\ m \in \mathbb{G}$ such that*

$$m(x_i, x_j) = (x_i', x_j')$$

Then same holds for side cubits.

Proof. Since the group $\mathbb{G}$ acts transitive on the cubits we know that $\exists\ m \in \mathbb{G}$ such that $m(x_j) = x_j'$. The trick is to find a move that sends x_j to x_j' without moving x_i then if $x_i \neq x_i'$ we need to find a move that sends x_i to x_i' without moving x_j'. By symmetry, one quickly sees that if we can send x_j to x_j' without moving x_i then this holds $\forall\ i$ so the second part follows. Since the group is symmetric, no generality is lost by choosing the start configuration and letting $x_i = x_1$. We will now send x_2 to all other corners without moving x_1:

- $x_2 \to x_3$: D^{-1}
- $x_2 \to x_4$: $L^{-1}D^{-1}$
- $x_2 \to x_5$: L^2D^{-1}
- $x_2 \to x_6$: D^2
- $x_2 \to x_7$: D
- $x_2 \to x_8$: BD

This can similarly be done with $x_3, \ldots, x_8$. Same with the side cubits, since the 6 basic moves also acts on them in a similar fashion. □

This shows that $\mathbb{G}$ acts 2-transitively on the unoriented cubits. To prove the theorem, we also need this for oriented cubits.

Lemma 3.3.4. *Let $c_i, c_j \in C_c$, where $c_i \neq c_j$. Let $c_i + 1$ be c_i with a clockwise twist and $c_i - 1$ be c_i with a counterclockwise twist. Then $\exists\ m \in \mathbb{G}$ such that*

$$m(c) = c \ \forall\ c \neq c_i \text{ and } c \neq c_j$$

and

$$m(c_i) = c_i + 1$$

and

$$m(c_j) = c_j - 1$$

or visa versa.
Further, let $c_i, c_j \in C_s$, where $c_i \neq c_j$. Let $c_i + 1$ be c_i with a clockwise twist. Then $\exists\ m \in \mathbb{G}$ such that

$$m(c) = c \ \forall\ c \neq c_i \text{ and } c \neq c_j$$

and

$$m(c_i) = c_i + 1$$

and

$$m(c_j) = c_j + 1$$

Proof. From lemma 3.3.3 we can change the position of any two pairs of unoriented cubits. There exists a move on the cube which only changes the orientation of two corner cubits, and leave all other cubits in place. It gives a $+1$ on one of the cubits and a -1 on the other. One such move is

$$m_0 = L^{-1}D^2LDL^{-1}DLRD^2R^{-1}D^{-1}RD^{-1}R^{-1}$$

which has disjoint cycle composition

$$[fdl, dlf, lfd][bld, dbl, ldb]$$

so it acts on c_2 and c_7, but by lemma 3.3.3 we can find $m \in \mathbb{G}$ such that

$$m(c_i, c_j) = (c_2, c_7)$$

and

$$m^{-1}m_0m \in \mathbb{H}$$

since $\mathbb{H}$ is normal. So $m^{-1}m_0m$ will only permute which two corners are being oriented and leave all others in their right place and orientation. There are also moves that changes the orientation of two side cubits without changing any other cubits. One such move is:

$$UR^{-1}LBR^{-1}LD^{-1}R^{-1}LF^{-1}R^{-1}LU^{-1}R^{-1}LB^{-1}R^{-1}LDR^{-1}LFR^{-1}L$$

which can more easily be described as $(U^{-1}M_F)^4(UM_F)^4$ with the definition of M_F from chapter 2. This will do the same trick for the side cubits. □

We can now prove Theorem 3.3.2

Proof. We have shown that if $m \in \mathbb{H}$, then $\zeta(\tau(m, S, x)) \equiv 0 \mod 3$ and $\zeta(\tau(m, S, y)) \equiv 0 \mod 2$. We have left to prove the converse. All we need to see is that $\dim \mathbb{H} = 7 \times 11$ since we know that $\mathbb{H} \cong L \subset (\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12})$ We will start with the corners. Lemma 3.3.4 gives me that $\exists\ m \in \mathbb{H}$ such that

$$\tau(m, S, \mathbf{x}) = (1, 0, \ldots, 0, -1)$$

for any position of 1, letting -1 be freezed to the last position. This gives us the following matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

where the rows are the twist vectors for the moves. These are linearly independent since $\det I_7 = 1 \neq 0$. The same can be done for the side cubits where we would end up with 11 row vectors where 1 would be freezed at the end and the first eleven columns would be the identity matrix. This shows that $\dim L = 7 \times 11 \Rightarrow L = K \Rightarrow K \cong \mathbb{H}$ □

This gives rise to the following exact sequence

$$0 \to \mathbb{H} \xrightarrow{\tau} (\mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}) \xrightarrow{\zeta} (\mathbb{Z}_3 \times \mathbb{Z}_2) \to 0$$

So if we look at $\phi : \mathbb{G} \to (S_8 \times S_{12})$ we have proven that

$$\mathbb{H} \cong \ker(\phi) \cong (\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11})$$

Remark 3.3.5. *If S had been a section such that $\tau(1, S, \mathbf{x}) = (0, \ldots, 1, \ldots, 0)$ then*

$$\sum_{x \in U(C_c)} \tau(m, S, x) \equiv 1 \mod 3$$

since the generators keep the sum equal to 0 modulo 3. Same for -1 and same for 1 modulo 2. If the cube was in the start configuration and you forced a twist on only one corner cubit (by using a screwdriver or something similar) then you would get into an orbit that you could not get out of. From this it should be plausible to conclude that the orientation of the group gives us $3 \cdot 2 = 6$ orbits of the configurations.

Chapter 4

Ω and permutations

We will now move our attention to the possible permutations of the unoriented cubits, leaving the subject of orientation for a while. I will assume some knowledge of cycles for this section.

4.1 Possible permutations

Looking at table 2.1 we can rewrite what happens to **x** and **y** in terms of cycle notation:

$$\begin{aligned}
\phi(D) &= [x_2, x_7, x_6, x_3][y_3, y_{12}, y_7, y_6] \\
\phi(U) &= [x_1, x_8, x_5, x_4][y_1, y_{10}, y_8, y_9] \\
\phi(F) &= [x_1, x_2, x_3, x_4][y_1, y_2, y_3, y_4] \\
\phi(B) &= [x_5, x_6, x_7, x_8][y_5, y_6, y_7, y_8] \\
\phi(L) &= [x_3, x_6, x_5, x_4][y_4, y_{11}, y_5, y_{10}] \\
\phi(R) &= [x_1, x_2, x_7, x_8][y_2, y_{12}, y_7, y_9]
\end{aligned}$$

So any $g \in G_6$ is a product of two odd permutations which is an even permutation. Since the product of two even permutations is even we have the following result:

Proposition 4.1.1. *Let $m \in \mathbb{G}$, then*

$$\text{sign}(\phi_c(m)) = \text{sign}(\phi_s(m))$$

Now, let $(\sigma_c, \sigma_s) \in (S_8 \times S_{12})$. Is it possible that $\text{sign}(\sigma_c) = \text{sign}(\sigma_s)$ but there is no $m \in \mathbb{G}$ such that $\phi_c(m) = \sigma_c$ and $\phi_s(m) = \sigma_s$?

Proposition 4.1.2. *Let* $(\sigma_c, \sigma_s) \in (S_8 \times S_{12})$ *and let* $sign(\sigma_c) = sign(\sigma_s)$. *Then* $\exists\ m \in \mathbb{G}$ *such that*

$$\phi_c(m) = \sigma_c \text{ and } \phi_s(m) = \sigma_s$$

Before this can be proven, we need some lemmas.

Lemma 4.1.3. *The alternating group,* A_n *is generated by 3-cycles.*

Proof. □

Lemma 4.1.4. $\mathbb{G}$ *acts 3-transitively on the unoriented corner and the side cubits respectively.*

Proof. This will be similar to the proof of Lemma 3.3.3. We now freeze two corners, e.g. x_1 and x_2 and see that we can move x_3 to any other corner.

- $x_3 \to x_4 : L^{-1}$
- $x_3 \to x_5 : L^2$
- $x_3 \to x_6 : L$
- $x_3 \to x_7 : B^2 L^2$
- $x_3 \to x_8 : B^{-1} L^2$

In order to prove this properly we should choose the two first corners in all possible positions, excluding symmetry. This would be a long and boring read and the reader who is familiar with the cube knows that this is not just possible, but rather easy. The side cubits will be the same with different moves. □

Lemma 4.1.5. $\forall\ x_i, x_j, x_k \in U(C_c)$ *where* $x_i \neq x_j \neq x_k$, *there* $\exists\ m \in \mathbb{G}$ *such that*

$$\phi(m) : [x_i, x_j, x_k]$$

and

$$m(x) = x$$

$\forall\ x \neq x_i, x_j, x_k$ *and*

$$m(y) = y$$

$\forall\ y \in U(C_s)$

Proof. In other words. It is possible to permute any three unoriented corner cubits without moving any other cubit. Now there exists a $m_0 \in \mathbb{G}$ such that

$$\phi(m_0) = [x_2, x_7, x_6]$$

and $m_0(c) = c$ for all other cubits. This move is:

$$m_0 = D^{-1}L^{-1}DRD^{-1}LDR^{-1}$$

which has cycle composition:

$$[frd, drb, ldb]$$

Since $\mathbb{G}$ is 3-transitive, $\exists\ m \in \mathbb{G}$ such that

$$m^{-1}m_0m$$

will permute any three corners, and leave all other cubits fixed. This is easy to see if you, for a particular $m \in \mathbb{G}$, write down the cycle notation for m and compute $m^{-1}m_0m$. □

Lemma 4.1.6. *$\forall\ y_i, y_j, y_k \in U(C_s)$ where $y_i \neq y_j \neq y_k$ $\exists\ m \in \mathbb{G}$ such that*

$$\phi(m) : [y_i, y_j, y_k]$$

and

$$m(y) = y$$

$\forall\ y \neq y_i, y_j, y_k$ and

$$m(x) = x$$

$\forall\ x \in U(C_s)$

Proof. This is analogue to the last lemma, so all we need is a $m \in \mathbb{G}$ that only permutes 3 side cubits without permuting anything else. One such move is

$$m_1 = F^{-1}D^2FDF^{-1}DFRD^2R^{-1}D^{-1}RD^{-1}R^{-1}$$

which has cycle composition

$$[fd, ld, rd]$$

□

Corollary 4.1.7. $(A_8 \times A_{12}) \subset \phi(\mathbb{G})$

Proof. Since A_n is generated by 3-cycles and all 3-cycles in A_8 and A_{12} can be realize as moves on the cube by Lemma 4.1.5 and Lemma 4.1.6, the corollary follows. □

We can now prove Proposition 4.1.2. Since $id_{S_n} = 1 \neq 0$ we will use $\xi_2 = (\{\pm 1\}, \cdot)$ instead of $\mathbb{Z}_2$. Keeping in mind that $\mathbb{Z}_2 \cong \xi_2$ by $f(a) = (-1)^a,\ a \in \mathbb{Z}_2$

Proof. We make the set

$$\Omega = \{(\sigma_c, \sigma_s) \in (S_8 \times S_{12}) \mid \text{sign}(\sigma_c) = \text{sign}(\sigma_s)\}$$

and want to prove that $\phi(\mathbb{G}) \cong \Omega$. We see that $(A_8 \times A_{12}) \subset \Omega$ and $\phi(\mathbb{G}) \subset \Omega$ from Proposition 4.1.1. We also have that

$$\Omega/(A_8 \times A_{12}) \cong \xi_2$$

since any $(\sigma_c, \sigma_s) \in \Omega$ is either $\text{sign}((\sigma_c, \sigma_s)) = (1, 1) \sim 1$ if $(\sigma_c, \sigma_s) \in (A_8 \times A_{12})$ or $\text{sign}((\sigma_c, \sigma_s)) = (-1, -1) \sim -1$. This gives rise to the exact sequences:

$$\begin{array}{ccccccccc}
 & & & & \{1\} & & \{1\} & & \\
 & & & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & A_8 \times A_{12} & \longrightarrow & \Omega & \longrightarrow & \xi_2 & \longrightarrow & \{1\} \\
 & & & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & A_8 \times A_{12} & \longrightarrow & S_8 \times S_{12} & \longrightarrow & \xi_2 \times \xi_2 & \longrightarrow & \{1\} \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \xi_2 & & \xi_2 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \{1\} & & \{1\} & &
\end{array}$$

Let $x, y \in \xi_2$, then $\xi_2 \times \xi_2$ goes to ξ_2 by xy, so ξ_2 is also the kernel where $x = y$. $S_8 \times S_{12}$ goes to $\xi_2 \times \xi_2$ by the sign homomorphism and $S_8 \times S_{12}$ goes to ξ_2 by $\text{sign}(x) \cdot (\text{sign}(y))^{-1}$. So

$$(A_8 \times A_{12}) \subset \phi(\mathbb{G}) \subset \Omega$$

by corollary 4.1.7, but

$$\Omega/(A_8 \times A_{12}) \cong \xi_2$$

so either

$$\phi(\mathbb{G}) \cong (A_8 \times A_{12})$$

or

$$\phi(\mathbb{G}) \cong \Omega$$

So all we need to find is a $m \in \mathbb{G}$ where $\text{sign}(\phi_c(m)) = \text{sign}(\phi_s(m)) = -1$, but this is true $\forall\, g \in G_6$ so

$$\phi(\mathbb{G}) \cong \Omega$$

which is equivalent to Proposition 4.1.2 □

We can now state the two Propositions in one Theorem

Theorem 4.1.8. *$m \in \mathbb{G}$ if and only if*

$$sign(\phi_c(m)) = sign(\phi_s(m))$$

Corollary 4.1.9.

$$\{1\} \longrightarrow \mathbb{H} \longrightarrow \mathbb{G} \xrightarrow{\phi} \Omega \longrightarrow \{1\}$$

is an exact sequence.

We now have the order of $\mathbb{G}$

Corollary 4.1.10.

$$|\mathbb{G}| = \frac{1}{2} \cdot 8! \cdot 12! \cdot 3^7 \cdot 2^{11} \approx 4.325 \cdot 10^{19}$$

Proof. Corollary 4.1.9 gives us that

$$\mathbb{G}/\mathbb{H} \cong \Omega \Rightarrow |\mathbb{G}|/|\mathbb{H}| = |\Omega| \Rightarrow |\mathbb{G}|/(3^7 \cdot 2^{11}) = \frac{1}{2} \cdot 8! \cdot 12!$$

□

When the first Rubik's cube came out an advertisement was made stating that the cube "has over 3 billion combinations but only one solution".[5] I would call that an understatement.

Remark 4.1.11. *If we apply the screwdriver method here again and force two cubits to be permuted while no other cubits were permuted then one would not be able to solve the cube. It seems that the rules of permutations gives us two orbits of configurations. Put together with the 6 from orientation it would be plausible to conclude that there are $2 \cdot 6 = 12$ orbits of the configuration of the cube. This also goes well with the fact that $|\mathbb{G}|$ was $\frac{1}{12}$ of the number of "possible" configurations on the cube.*

4.2 Ω to action!

How does Ω act on $\mathbb{H}$? Not directly, naturally, since $\mathbb{H} \subset \mathbb{G}$ and $\Omega \subset (S_8 \times S_{12})$. We will need the following:

Lemma 4.2.1. *For $m, m' \in \mathbb{G}$ and $m \neq m'$ and $h \in \mathbb{H}$ let $\phi(m) = \phi(m')$ then*

$$m^{-1}hm = m'^{-1}hm'$$

Proof. Since $\phi(m) = \phi(m') = \sigma$ the only difference between m and m' lies in the orientation. We will let c_i be a corner or side cubit and let $c_i + 1$ the the same cubit rotated clockwise and $c_i - 1$ be a counterclockwise rotation. Now, let m and m' send c_i to c_j, but let $m(c_i) = c_j$ and $m'(c_i) = c_j + 1$. Let h change orientation by $+1$ (this could be any change). Then

$$m^{-1}hm(c_i) = m^{-1}h(c_j) = m^{-1}(c_j + 1) = c_i + 1$$

and

$$m'^{-1}hm'(c_i) = m'^{-1}h(c_j + 1) = m'^{-1}(c_j + 2) = c_i + 1$$

since m'^{-1} will add a -1. □

So the choice of m is irrelevant as long as $\phi(m) = \phi(m')$. We will therefore write $\sigma^{-1}h\sigma$ where σ"="m for any m such that $\phi(m) = \sigma$. We will now look at the map: $\sigma(h) = \sigma^{-1}h\sigma$.

Lemma 4.2.2.

$$\sigma(\mathbb{H}) \subset Aut(\mathbb{H})$$

Proof. So we have to show that σ is a homomorphism on elements of $\mathbb{H}$ and that $\sigma : \mathbb{H} \to \mathbb{H}$ is injective. Let $h_1, h_2 \in \mathbb{H}$. Then

$$\sigma(h_1h_2) = \sigma^{-1}(h_1h_2)\sigma = \sigma^{-1}h_1\sigma^{-1}\sigma h_2\sigma = \sigma(h_1)\sigma(h_2)$$

so σ is a homomorphism. Since $\mathbb{H}$ is normal we know that $\sigma^{-1}h\sigma \in \mathbb{H}$ so $\exists\ h' \in \mathbb{H}$ such that

$$h' = \sigma^{-1}h\sigma$$

for any given $h \in \mathbb{H}$. Hence $\sigma \subset Aut(\mathbb{H})$ □

So Ω simply permutes the elements in $\mathbb{H}$ by conjugation.

Proposition 4.2.3. *$\mu : \Omega \to Aut(\mathbb{H})$ given by*

$$\mu_h(\sigma) = \sigma^{-1}h\sigma$$

for any $h \in \mathbb{H}$ is a homomorphism.

Proof.

$$(\mu_h(\sigma_2)(\sigma_1)) = \mu(\sigma_2)(\sigma_1^{-1}h\sigma_1) = \sigma_2^{-1}\sigma_1^{-1}h\sigma_1\sigma_2 = (\sigma_1\sigma_2)^{-1}h\sigma_1\sigma_2 = \mu_h(\sigma_1\sigma_2)$$

□

4.3 Semidirect product

Definition 4.3.1. *Let N and A be two groups and let $\phi : A \to Aut(N)$ be a homomorphism with $a_1, a_2 \in A$ and $n_1, n_2 \in N$ We define a product*

$$\odot : ((N \times A) \times (N \times A)) \to (N \times A)$$

by

$$\odot((n_1, a_1), (n_2, a_2)) = (n_1 \phi_{a_1}(n_2), a_1, a_2)$$

Lemma 4.3.2.

$$((N \times A), \odot)$$

Is a group called the semidirect product *of N and A with regard to ϕ and is a group. It is denoted by*

$$N \rtimes_\phi A$$

Proof. [3] on p. 162. Sketch: The identity is (id_N, id_A) and

$$(n, a)^{-1} = (\phi_{a^{-1}}(n^{-1}), a^{-1})$$

□

It is worth noting that pairs (n, id_A) form a normal subgroup of the product isomorphic to N, and pairs (id_N, a) form a subgroup of the product isomorphic to A. So if we have two groups and a certain homomorphism, we can create this product. We can also start with a group, and if it has certain properties it can be written as a semidirect product.

Lemma 4.3.3. *Let G be a group with N as a normal subgroup. If $\exists\ A \subset G$ where $G = NA$ and $N \cap A = 1$ then $\exists$ some homomorphism $\phi : A \to Aut(N)$ such that*

$$G \cong N \rtimes_\phi A$$

Proof. See Lemma 7.20 on p. 168 in [4]. □

Can $\mathbb{G}$ be written as a semidirect product? $\mathbb{H}$ is normal and if $\Omega \cong A \subset \mathbb{G}$ then $\mathbb{H} \cap A = 1$. We can use μ as our homomorphism. All we have to check is that $\exists\ A \subset \mathbb{G}$ such that $A \cong \Omega$ and that $\mathbb{G} = \mathbb{H}A$

Lemma 4.3.4. *The set*

$$A = \{m \in \mathbb{G} \mid \tau(m, S, x) = 0\ \forall\ x \in U(C)\}$$

is a subgroup of $\mathbb{G}$.

Proof. The identity is carried over so we need to check that if $m, n \in A$ then $mn \in A$. We use corollary 4.2.3 and since $m^{-1}x \in U(C_c)$ then

$$\tau(mn, S, x) = \tau(m, S, x) + \tau(n, S, m^{-1}x) = 0 + 0 = 0 \tag{4.1}$$

so $mn \in A$. Same argument works for the sides. Now we have to show that if $m \in A$ then $m^{-1} \in A$. Since $\mathbb{G}$ is a finite group, then for each $m \in \mathbb{G}\ \exists\ a \in \mathbb{N}$ such that

$$m^a = 1$$

(since $\langle m \rangle$ is a subgroup of $\mathbb{G}$). So let $m \in A$ and $m^a = 1$ then $m^{a-1} = m^{-1}$ and

$$\tau(m^{a-1}, S, x) = 0$$

by induction of equation (4.1), so $m^{-1} \in A$ □

Lemma 4.3.5.

$$A \cong \Omega$$

Proof. Now we need to show that for each $\sigma \in \Omega$, $\exists\ m \in A$ such that $\phi(m) = \sigma$. Let us first look at any $m \in \mathbb{G}$. Then $\phi(m) = \sigma$. Now if $\tau(m, S, \mathbf{x}) = \mathbf{0}$ we are done, so let's assume $\tau(m, S, \mathbf{x}) \neq \mathbf{0}$. Let $h \in \mathbb{H}$. Then

$$\tau(hm, S, x) = \tau(h, S, x) + \tau(m, S, x)$$

because $hx = x$. So since $\mathbb{H} \cong (\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11})$ and $\zeta(\tau(m, S, x)) \equiv 0 \mod 3$ for corners and $\zeta(\tau(m, S, y)) \equiv 0 \mod 2$ for sides, then for each $m \in \mathbb{G}\ \exists\ h \in \mathbb{H}$ such that $\tau(hm, S, x) = 0\ \forall\ x \in U(C)$. So $hm \in A$. □

Theorem 4.3.6.

$$\mathbb{G} \cong \mathbb{H} \rtimes_\mu \Omega$$

Proof. All that is left now is to see that $\mathbb{G} = \mathbb{H}A$. This is just the same argument as in Lemma 3.1.4. Each move can be realized as first a change in orientation and then a permutation. So $\forall\ m \in \mathbb{G}, \exists!\ h \in \mathbb{H}, \alpha \in A$ such that $m = \alpha h$. □

$\mathbb{G}$ is now completely mapped.

Chapter 5

The center, $Z(\mathbb{G})$

Definition 5.0.7.

$$Z(G) = \{x \in G \mid gx = xg \ \forall \ g \in G\}$$

is called the center *of the group G.*

It is easy to see that $Z(G)$ is a subgroup of G, and it will not be proven here. So what is $Z(\mathbb{G})$? It turns out it's not much. Proving this, however, is now fairly easy because of our knowledge of $\mathbb{H}$.

Lemma 5.0.8.

$$Z(\mathbb{G}) \subset \mathbb{H}$$

Proof. Let $m \in Z(\mathbb{G})$ but $m \notin \mathbb{H}$. Then m permutes some $c_i \in C$. So $\phi(m) \in (S_8 \times S_{12})$ and is not trivial, but $Z(S_8 \times S_{12})$ is trivial since $Z(S_n)$ is trivial $\forall \ n > 2$. □

Lemma 5.0.9. *Let $m \in Z(\mathbb{G})$ and $m \neq 1$. Then m must either change the orientation of all side cubits, or m must change the orientation of all the corner cubits.*

Proof. Let $m \in \mathbb{H}$. Then m changes the orientation of some cubit c_i to c_i', ($c_i \neq c_i'$) so $m(c_i) = c_i'$. Let m not change orientation of c_j. Since $\mathbb{G}$ acts 2-transitively, $\exists \ g \in \mathbb{G}$ such that $g(c_i) = c_j$. Then $g(c_i') = c_j'$ where c_j' is c_j with a new orientation. This gives

$$gm(c_i) = g(c_i') = c_j'$$

and

$$mg(c_i) = m(c_j) = c_j$$

so $m \notin Z(\mathbb{G})$. Hence for m to be in $Z(\mathbb{G})$, m must change the orientation of all the cubits, and since the side cubits and the corner cubits acts separately the result follows. □

Proposition 5.0.10.

$$Z(\mathbb{G}) = \{m_s, 1\}$$

where m_s is the move that changes orientation of all the side cubits.

Proof. We see that m must change the orientation of all the side or all the corner cubits. If m_s changes the orientation of all side cubits then $\tau(m_s, S, \mathbf{y}) = (1,1,1,1,1,1,1,1,1,1,1,1)$ and $\zeta(\tau(m_s, S, y)) \equiv 0 \mod (2)$, so m_s is a move that can be realized on the cube. The corner cubits gives more difficulty since they can be oriented in two ways. So not only must m change the orientation of all the corner cubits, it must change all of them either clockwise or counter clockwise. Let m_c change all the cubits clockwise and let S be the section that gives the value 1 for clockwise change and -1 for counterclockwise change. Then $\tau(m_c, S, \mathbf{x}) = (1,1,1,1,1,1,1,1)$ and $\zeta(\tau(m, S, y)) \equiv -1 \mod (3)$, and hence m_c is not a move in $\mathbb{H}$ by Theorem 3.3.2. If $m_{c'}$ changes all the orientation counterclockwise then

$$m_c m_{c'} = 1 \iff m_{c'} = m_c^{-1}$$

and since $Z(\mathbb{G})$ is a group then $m_{c'} \notin Z(\mathbb{G})$. □

The move m_s applied to the start configuration is often called the "superflip" configuration. It was the first configuration proven to need at least 20 letters to achieve from the start configuration.[1]

[1]See appendix A

Chapter 6

How to solve the cube.

I would recommend getting a Rubik's cube for this section. We will not go about trying to explain how to "speed-solve" the cube, but rather lay out a methodical way. Much of the moves that will be used has already been introduced earlier in the thesis. The U, D, R, L, F, L notation will be used, but the explicit moves are not so important as the general ideas. We will also start to use the M_F, M_R, M_M notations. The M_F move is moving the middle row vertically $90°$ through F, U, B, D faces. It is rotated the same way as R, not as L. M_R is the other middle vertical that go through the R, U, L, D faces. It is rotated the same way as the F face, not as B. The M_M is moving the horizontal middle row, the one that goes through the F, R, B, L faces. It is rotated the same way as D face and not as U. Remember to read all the moves from right to left.

6.1 Solving one face

We start by solving one of the 6 faces. This is relatively easy. It is not enough, however to just solve one face, it must be solved in the "right way" since you have to solve the rest of the cube also. I will illustrate the right way in figure 6.1. If stuck on the first side, one can use the moves outlined in the last section of this chapter and make them fit your configuration by conjugation.

6.2 Solving the second row.

Let the cube be rotated so the solved side is on the top, and make sure your center pieces is on the right faces. The next step will be get all the side cubits on the second row right. See figure 6.2. That is, to place the fr, fl, br, bl

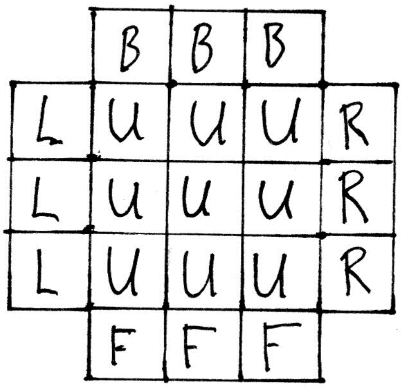


Figure 6.1: 'Up' face solved the right way

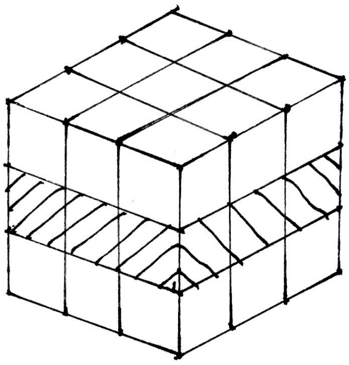


Figure 6.2: Second row

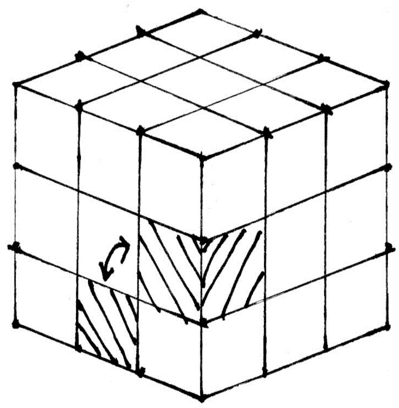


Figure 6.3: Solving the second row

cubits right. The trick is to find a move that swaps side cubits on the second row with side cubits on the bottom. This move is very easy, and it will only mess up bottom cubits without ruining our top. First you find a side cubit on the bottom that you want to place on the second row. You do D some times so the side cubit's color at the bottom is the same as the center color of that face. See figure 6.3. If you want to swap fd with fr you do:

$$F^1D^{-1}FDRDR^{-1}D^{-1}$$

If you want to swap fd with fl you do:

$$FD^{-1}F^{-1}D^{-1}L^{-1}D^{-1}LD$$

You repeat this until all the second row side cubits are correct. If there are two swapped second row side cubits, you can take one down by permuting it with a random side cubit from the bottom and then permute it up at the right location. The same technique can be used if a side cubit is in its right cubicle but in the wrong orientation.

6.3 The side cubits of the bottom

Two things remain before the whole cube is solved, the bottom and the third row. We shall proceed to solve the bottom and then solve the third row at last. We start with the side cubits. Now, there is a move which as disjoint

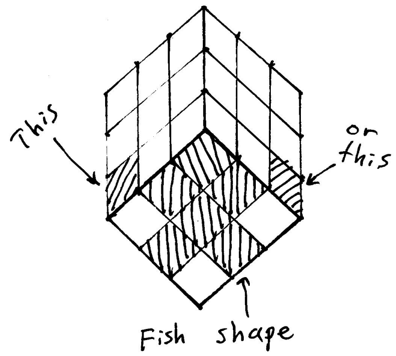


Figure 6.4: The fish.

cycle composition

$$[fd, bf][ld, dr]$$

so it permutes and change orientation of four side cubits without moving anything else. Now do D some times until the cube in the desired position according to the cycle composition of this move and then do:

$$M_F D M_F^{-1} D M_F D M_F^{-1} D M_F D M_F^{-1}$$

If not all the side cubits face down one can do D unitill the cubits line up with the cycle composition and then do the move again. It should be possible to get all the side cubits at the bottom in the right orientation through this process. Just keep a close eye on the cycle composition.

6.4 Finishing the bottom

All that is left now is permuting and switching orientation of at most 8 cubits. The bottom side cubits should all face down now. The goal now is to create a "fish" shape. See figure 6.4. To create this you do the "fish" move: $RD^2R^{-1}D^{-1}RD^{-1}R^{-1}$, which has cycle notation:

$$[frd, dbl, rdf][fdl, bdr, lfd][ld, bd, rd]$$

This is the "right" fish move. The left is analogous: $L^{-1}D^2LDL^{-1}DL$, with cycle notation:

$$[frd, bld, rdf][fdl, drb, lfd][ld, rd, bd]$$

The fish move is applied to F, B, R or L if one let the 'up' face be the one that was solved first. What of these faces chosen as the new front face depends on the cubes configuration. After doing this some times one should end up with a fish shape at the bottom. When this is achieved one can do the fish move on the face that has a cubit sharing the same color as the fish closest to the fish's "head". See figure 6.4. One does the "right" move if it is a right corner cubit and the "left" move if it is a left corner cubit. The bottom should now be solved, but most likely not in the "right way" so there is still have some work to do with the third row.

6.5 Finishing the rest

The cube is now nearly done. The bottom looks fine but some of the cubits might still be in the wrong position with regard to the third row. We now need a set of moves that permutes cubits without rotating them so the bottom stays the same. We will just present some basic moves that are usefull with their cycle notation, and one should be able to finish the rest. Remember to use conjugation if needed to move some other cubits than the ones in the cycle notation. Be carefull to memorize or write the moves done on the cube before one of these moves so it can be easy to do the inverse afterwards.

- Permuting three sides:

$$F^{-1}D^2FDF^{-1}DFRD^2R^{-1}D^{-1}RD^{-1}R^{-1}$$

  cycle notation:

$$[fd, ld, rd]$$

- Permuting three corners:

$$BD^{-1}F^{-1}DB^{-1}D^2FD^{-1}F^{-1}D^2FL^{-1}DRD^{-1}LD^2R^{-1}DRD^2R^{-1}$$

  cycle notation:

$$[fdl, rdf, bdr]$$

- Orienting two sides:

$$(U^{-1}M_F)^4(UM_F)^4$$

  cycle notation:

$$[ul, lu][ur, ru]$$

- Permuting two corners and two sides:

$$L^{-1}DRD^{-1}LD^2R^{-1}DRD^2R^{-1}$$

  cycle notation:

$$[frd, rbd][fd, rd]$$

Appendix A

God's number

If one had the capacity to solve the Rubik's cube in the most efficient of ways, how many moves would you need? It turns out that the answer is 20 if we allow $g^2 \ \forall \ g \in G_6$. No more than 20 moves are needed to solve the cube and hence no more than 40 moves are needed to get from one configuration to any other configuration. I have chosen to include table A.1 from [2].

Proposition A.0.1. *No $m \in \mathbb{G}$ need to be longer than 20 letters.*

Proof. It has been proven that it takes no more than 20 letters to go from any configuration to the start configuration. This proposition is a bit stronger, it states that it takes no more than 20 letters to get from one configuration to any other configuration. Let l be any valid configuration and define this to be the (new) start configuration. If one applies the moves needed to go from the start configuration to all the configurations in the table above one would end up at new configurations, but they would all be 20 or less letter away from l and they would all be included since no two different moves give the same configuration. This can be done for any configuration. □

The "superflip" from the Center is one of the moves that creates a configuration that takes no less than 20 letters to solve. It was actually the first move proven to take no less than 20 letters to solve. This move does it in exactly 20 letters [2]:

$$UR^2UF^2DR^2UB^{-1}F^{-1}U^2LB^2R^2F^2DU^{-1}FU^2LR$$

Distance	Number of configurations
0	1
1	18
2	243
3	3240
4	43 239
5	574 908
6	7 618 438
7	100 803 036
8	1 332 343 288
9	17 596 479 795
10	232 248 063 316
11	3 063 288 809 012
12	40 374 425 656 248
13	531 653 418 284 628
14	6 989 320 578 825 358
15	91 365 146 187 124 313
16	ca. $1,1 \cdot 10^{18}$
17	ca. $1.2 \cdot 10^{19}$
18	ca. $2,9 \cdot 10^{19}$
19	ca. $1,5 \cdot 10^{18}$
20	ca. $3 \cdot 10^{9}$

Table A.1:

Bibliography

[1] Fragleigh, John B., *A first course in Abstract Algebra*, seventh ed., Pearson Education, Inc. 2003.

[2] *God's number is 20*, http://www.cube20.org/

[3] Joyner, W. D., *Mathematics of the Rubik's Cube*. Available at: www.permutationpuzzles.org/rubik/webnotes/rubik.pdf Accessed 16. May 2012.

[4] Rotman, Joseph J., *An Introduction to the Theory of Groups*, fourth ed., Springer-Verlag New York, Inc. 1995.

[5] Rubik's cube commercial from 1981. Can be found at http://www.youtube.com/watch?v=jTkhA3RO5fU Accessed 1. May 2012

[6] Weiss, Michael, *More Ru-brik-a-brac*, available at: http://www.math.niu.edu/∼rusin/known-math/95/rubik.physics Accessed 15. March 2012.