Group Theory

Rubik's Cube and the Permutation Group

Mohammed Alshamsi

2021004826

mo.alshamsi@aurak.ac.ae

Coding Club at the American University of Ras Al Khaimah

September 29, 2024

Introduction

- Group Theory?

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?**

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes
- **Why Math?**

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes
- **Why Math?** You'll learn new ways of reasoning, which will enable you to make more sophisticated software.

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes
- **Why Math?** You'll learn new ways of reasoning, which will enable you to make more sophisticated software.
- **These Slides?**

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes
- **Why Math?** You'll learn new ways of reasoning, which will enable you to make more sophisticated software.
- **These Slides?** See our GitHub repository.

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes
- **Why Math?** You'll learn new ways of reasoning, which will enable you to make more sophisticated software.
- **These Slides?** See our GitHub repository.
- **Coding Background?**

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes
- **Why Math?** You'll learn new ways of reasoning, which will enable you to make more sophisticated software.
- **These Slides?** See our GitHub repository.
- **Coding Background?** Check GitHub or find a guide online. (We won't need it in this presentation.)

Introduction

- **Group Theory?** Study of groups (abstract algebraic structures)
- **Format?** You'll see the following:
  - Mathematical definitions with examples
  - Applications to Rubik's cubes
- **Why Math?** You'll learn new ways of reasoning, which will enable you to make more sophisticated software.
- **These Slides?** See our GitHub repository.
- **Coding Background?** Check GitHub or find a guide online. (We won't need it in this presentation.)

Any questions?

Outline

Review of Sets

Example (Familiar Sets)

Example (Familiar Sets)

$$\{0, 1, 2, 3, \ldots\} = \mathbb{N} \qquad \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$$

Example (Familiar Sets)

$$\{0, 1, 2, 3, \ldots\} = \mathbb{N} \qquad \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$$

$$\left\{\frac{p}{q} : p, q \in \mathbb{Z}\right\} = \mathbb{Q}$$

Example (Familiar Sets)

$$\{0, 1, 2, 3, \dots\} = \mathbb{N} \qquad \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$$

$$\left\{\frac{p}{q} : p, q \in \mathbb{Z}\right\} = \mathbb{Q}$$

Definition

Review of Sets

Example (Familiar Sets)

$$\{0, 1, 2, 3, \dots\} = \mathbb{N} \qquad \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$$

$$\left\{\frac{p}{q} : p, q \in \mathbb{Z}\right\} = \mathbb{Q}$$

Definition

Union: $A \cup B$, all elements that are in A or B

Review of Sets

Example (Familiar Sets)

$$\{0, 1, 2, 3, \dots\} = \mathbb{N} \qquad \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$$

$$\left\{\frac{p}{q} : p, q \in \mathbb{Z}\right\} = \mathbb{Q}$$

Definition

Union: $A \cup B$, all elements that are in A or B

Intersection: $A \cap B$, all elements that are in A and B

Review of Sets

Example (Familiar Sets)

$$\{0, 1, 2, 3, \dots\} = \mathbb{N} \qquad \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$$

$$\left\{ \frac{p}{q} : p, q \in \mathbb{Z} \right\} = \mathbb{Q}$$

Definition

Union: $A \cup B$, all elements that are in A or B

Intersection: $A \cap B$, all elements that are in A and B

Subtraction: $A - B$, all elements in A that are not in B

Review of Sets

Example (Familiar Sets)

$$\{0, 1, 2, 3, \ldots\} = \mathbb{N} \qquad \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$$

$$\left\{\frac{p}{q} : p, q \in \mathbb{Z}\right\} = \mathbb{Q}$$

Definition

Union: $A \cup B$, all elements that are in A or B

Intersection: $A \cap B$, all elements that are in A and B

Subtraction: $A - B$, all elements in A that are not in B

Subset: $B \subseteq A$, all elements of B are in A.

Functions

Definition (Function)

Functions

Definition (Function)

$f : X \to Y$, rule that assigns to each element of X exactly one element of Y.

This is denoted $f(x)$

Functions

Definition (Function)

$f : X \to Y$, rule that assigns to each element of X exactly one element of Y.

This is denoted $f(x)$

Definition (Operation)

Functions

Definition (Function)

$f : X \to Y$, rule that assigns to each element of X exactly one element of Y.
This is denoted $f(x)$

Definition (Operation)

$* : X \times X \to X$, assigns to each pair of elements x, y from X an element of X.
This is denoted $x * y$

Definition (Group)

Groups

Definition (Group)

Set G and an operation $* : G \times G \rightarrow G$, where:

Groups

Definition (Group)

Set G and an operation $* : G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$

Definition (Group)

Set G and an operation $* : G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$

Definition (Group)

Set G and an operation $*: G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Groups

Definition (Group)

Set G and an operation $* : G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Example ($\mathbb{Z}$ under addition)

Groups

Definition (Group)

Set G and an operation $* : G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Example ($\mathbb{Z}$ under addition)

1. Addition is associative; $(a + b) + c = a + (b + c)$

Groups

Definition (Group)

Set G and an operation $*: G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Example ($\mathbb{Z}$ under addition)

1. Addition is associative; $(a + b) + c = a + (b + c)$
2. Identity element is 0

Groups

Definition (Group)

Set G and an operation $*: G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Example ($\mathbb{Z}$ under addition)

1. Addition is associative; $(a + b) + c = a + (b + c)$
2. Identity element is 0
3. Every element's inverse is its negative

Groups

Definition (Group)

Set G and an operation $*: G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Example ($\mathbb{Z}$ under addition)

1. Addition is associative; $(a + b) + c = a + (b + c)$
2. Identity element is 0
3. Every element's inverse is its negative

$\mathbb{Z}$ is a group under addition!

Groups

Definition (Group)

Set G and an operation $*: G \times G \to G$, where:

1. $*$ is associative; $(a * b) * c = a * (b * c)$
2. There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Example ($\mathbb{Z}$ under addition)

1. Addition is associative; $(a + b) + c = a + (b + c)$
2. Identity element is 0
3. Every element's inverse is its negative

$\mathbb{Z}$ is a group under addition!

Notational shortcut: ab instead of $a * b$.

Group Example

Example (Integers modulo 12)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Group Example

Example (Integers modulo 12)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Operation: Clock arithmetic. $8 + 9 = 5 \pmod{12}$, for example.

Group Example

Example (Integers modulo 12)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Operation: Clock arithmetic. $8 + 9 = 5 \pmod{12}$, for example.

1. Associativity?

Group Example

Example (Integers modulo 12)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Operation: Clock arithmetic. $8 + 9 = 5 \pmod{12}$, for example.

1. Associativity?
2. Identity?

Group Example

Example (Integers modulo 12)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Operation: Clock arithmetic. $8 + 9 = 5 \pmod{12}$, for example.

1. Associativity?
2. Identity?
3. Inverses?

Group Example

Example (Integers modulo 12)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Operation: Clock arithmetic. $8 + 9 = 5 \pmod{12}$, for example.

1. Associativity?
2. Identity?
3. Inverses?

It's a group.

Theorem (Group Properties)

Theorem (Group Properties)

- Identity is unique

Theorem (Group Properties)

- Identity is unique
- Cancellation law: $ab = ac \implies b = c$, and $ba = ca \implies b = c$

Theorem (Group Properties)

- Identity is unique
- Cancellation law: $ab = ac \implies b = c$, and $ba = ca \implies b = c$
- Exactly one inverse per element

Groups

Theorem (Group Properties)

- Identity is unique
- Cancellation law: $ab = ac \implies b = c$, and $ba = ca \implies b = c$
- Exactly one inverse per element
- Inverse of ab is $b^{-1}a^{-1}$

Integers modulo 12

Definition (Subgroup)

Integers modulo 12

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation. "$H \leqslant G$" means "H is a subgroup of G".

Integers modulo 12

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation. "$H \leqslant G$" means "H is a subgroup of G".

Example (Subgroups of $\mathbb{Z}_{12}$)

Integers modulo 12

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation. "$H \leqslant G$" means "H is a subgroup of G".

Example (Subgroups of $\mathbb{Z}_{12}$)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \quad \text{and} \quad \{0\}$$

Integers modulo 12

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation. "$H \leqslant G$" means "H is a subgroup of G".

Example (Subgroups of $\mathbb{Z}_{12}$)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \quad \text{and} \quad \{0\}$$

$$\{0, 6\}$$

Integers modulo 12

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation. "H $\leqslant$ G" means "H is a subgroup of G".

Example (Subgroups of $\mathbb{Z}_{12}$)

$$\{0,1,2,3,4,5,6,7,8,9,10,11\} \quad \text{and} \quad \{0\}$$

$$\{0,6\}$$

$$\{0,4,8\}$$

Integers modulo 12

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation. "H $\leqslant$ G" means "H is a subgroup of G".

Example (Subgroups of $\mathbb{Z}_{12}$)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \quad \text{and} \quad \{0\}$$

$$\{0, 6\}$$

$$\{0, 4, 8\}$$

$$\{0, 3, 6, 9\}$$

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation. "$H \leqslant G$" means "H is a subgroup of G".

Example (Subgroups of $\mathbb{Z}_{12}$)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \quad \text{and} \quad \{0\}$$

$$\{0, 6\}$$

$$\{0, 4, 8\}$$

$$\{0, 3, 6, 9\}$$

$$\{0, 2, 4, 6, 8, 10\}$$

Theorem (Basic Properties of Subgroups)

Basic Properties of Subgroups

Theorem (Basic Properties of Subgroups)

- A subgroup H of a group G always contains the identity.

Basic Properties of Subgroups

Theorem (Basic Properties of Subgroups)

- A subgroup H of a group G always contains the identity.
- The inverse of any $h \in H$ is the same as in G, and is also a part of H.

Integers modulo 12

Definition (Generating Set)

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.
The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Example (Generators in $\mathbb{Z}_{12}$)

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Example (Generators in $\mathbb{Z}_{12}$)

1 generates $\mathbb{Z}_{12}$.

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S\rangle$.

Example (Generators in $\mathbb{Z}_{12}$)

1 generates $\mathbb{Z}_{12}$.

2 generates $\{0, 2, 4, 6, 8, 10\}$.

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Example (Generators in $\mathbb{Z}_{12}$)

1 generates $\mathbb{Z}_{12}$.

2 generates $\{0, 2, 4, 6, 8, 10\}$.

3 generates:

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Example (Generators in $\mathbb{Z}_{12}$)

1 generates $\mathbb{Z}_{12}$.

2 generates $\{0, 2, 4, 6, 8, 10\}$.

3 generates:

4 generates:

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Example (Generators in $\mathbb{Z}_{12}$)

1 generates $\mathbb{Z}_{12}$.

2 generates $\{0, 2, 4, 6, 8, 10\}$.

3 generates:

4 generates:

6 generates:

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G's operation) of the elements of S and their inverses, forms a subgroup of G.

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Example (Generators in $\mathbb{Z}_{12}$)

1 generates $\mathbb{Z}_{12}$.

2 generates $\{0, 2, 4, 6, 8, 10\}$.

3 generates:

4 generates:

6 generates:

What is $\langle 5 \rangle$?

Cosets

Definition (Coset)

Cosets

Definition (Coset)

For each element g of G, there exists a *(right) coset* of H in G, defined as follows:

$$Hg = \{hg : h \in H\}$$

Cosets

Definition (Coset)

For each element g of G, there exists a *(right) coset* of H in G, defined as follows:

$$Hg = \{hg : h \in H\}$$

Example (Right Cosets in $\mathbb{Z}_{12}$)

Cosets

Definition (Coset)

For each element g of G, there exists a *(right) coset* of H in G, defined as follows:

$$Hg = \{hg : h \in H\}$$

Example (Right Cosets in $\mathbb{Z}_{12}$)

$\{1, 3, 5, 7, 9, 11\}$ is a coset of $\langle 2 \rangle$. We can denote it by $\langle 2 \rangle + 1$, $\langle 2 \rangle + 3$, et cetera. (They're all the same coset!)

Cosets

Definition (Coset)

For each element g of G, there exists a *(right) coset* of H in G, defined as follows:

$$Hg = \{hg : h \in H\}$$

Example (Right Cosets in $\mathbb{Z}_{12}$)

$\{1, 3, 5, 7, 9, 11\}$ is a coset of $\langle 2 \rangle$. We can denote it by $\langle 2 \rangle + 1$, $\langle 2 \rangle + 3$, et cetera. (They're all the same coset!)

Cosets of $\langle 3 \rangle$ are $\langle 3 \rangle + 1$ and $\langle 3 \rangle + 2$.

Cosets

Definition (Coset)

For each element g of G, there exists a *(right) coset* of H in G, defined as follows:

$$Hg = \{hg : h \in H\}$$

Example (Right Cosets in $\mathbb{Z}_{12}$)

$\{1, 3, 5, 7, 9, 11\}$ is a coset of $\langle 2 \rangle$. We can denote it by $\langle 2 \rangle + 1$, $\langle 2 \rangle + 3$, et cetera. (They're all the same coset!)

Cosets of $\langle 3 \rangle$ are $\langle 3 \rangle + 1$ and $\langle 3 \rangle + 2$.

Cosets of $\langle 4 \rangle$ are:

Definition (Coset)

For each element g of G, there exists a *(right) coset* of H in G, defined as follows:

$$Hg = \{hg : h \in H\}$$

Example (Right Cosets in $\mathbb{Z}_{12}$)

$\{1, 3, 5, 7, 9, 11\}$ is a coset of $\langle 2 \rangle$. We can denote it by $\langle 2 \rangle + 1$, $\langle 2 \rangle + 3$, et cetera. (They're all the same coset!)

Cosets of $\langle 3 \rangle$ are $\langle 3 \rangle + 1$ and $\langle 3 \rangle + 2$.

Cosets of $\langle 4 \rangle$ are:

Cosets of $\langle 6 \rangle$ are:

Theorem (Properties of Cosets)

Cosets

Theorem (Properties of Cosets)

- Hg_1 and Hg_2, for any g_1 and g_2, are either the same coset or are completely disjoint.

Cosets

Theorem (Properties of Cosets)

- Hg_1 and Hg_2, for any g_1 and g_2, are either the same coset or are completely disjoint.
- All cosets of H, including H itself (He), are the same size.

Cosets

Theorem (Properties of Cosets)

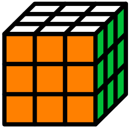
- Hg_1 and Hg_2, for any g_1 and g_2, are either the same coset or are completely disjoint.
- All cosets of H, including H itself (He), are the same size.
- The union of all cosets of H produces the group set of G.

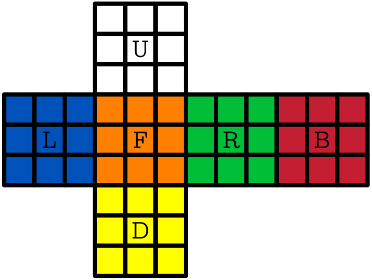
Cosets

Theorem (Properties of Cosets)

- Hg_1 and Hg_2, for any g_1 and g_2, are either the same coset or are completely disjoint.
- All cosets of H, including H itself (He), are the same size.
- The union of all cosets of H produces the group set of G.
- (Lagrange's Theorem) The number of cosets, $(G : H)$, is equal to $\frac{|G|}{|H|}$.

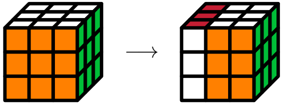
Here's a Rubik's Cube:

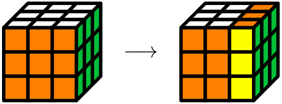


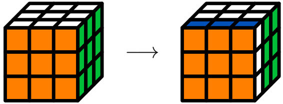


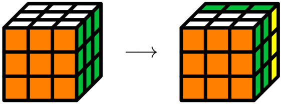
The Rubik's Cube Group

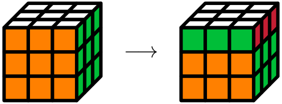
The group is generated by the following set of rotations:

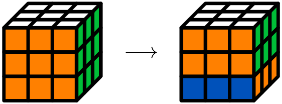
L:


R:


F:


B:


U:


D:


This group has $2^{27}3^{14}5^{3}7^{2}11 = 43,252,003,274,489,856,000$ elements!

Nested Subgroups of the Rubik's Cube Group

The Rubik's Cube group G may be split into these subgroups:

Nested Subgroups of the Rubik's Cube Group

The Rubik's Cube group G may be split into these subgroups:

$$G_0 = \langle L, R, F, B, U, D \rangle \qquad |G_0| = 4.3 \times 10^{19}$$

$$G_1 = \langle L, R, F, B, U^2, D^2 \rangle \qquad |G_1| = 2.1 \times 10^{16}$$

$$G_2 = \langle L, R, F^2, B^2, U^2, D^2 \rangle \qquad |G_2| = 1.9 \times 10^{10}$$

$$G_3 = \langle L^2, R^2, F^2, B^2, U^2, D^2 \rangle \qquad |G_3| = 6.6 \times 10^5$$

$$G_4 = \langle 1 \rangle \qquad |G_4| = 1$$

Nested Subgroups of the Rubik's Cube Group

The Rubik's Cube group G may be split into these subgroups:

$$\begin{aligned}
G_0 &= \langle L, R, F, B, U, D \rangle & |G_0| &= 4.3 \times 10^{19} \\
G_1 &= \langle L, R, F, B, U^2, D^2 \rangle & |G_1| &= 2.1 \times 10^{16} \\
G_2 &= \langle L, R, F^2, B^2, U^2, D^2 \rangle & |G_2| &= 1.9 \times 10^{10} \\
G_3 &= \langle L^2, R^2, F^2, B^2, U^2, D^2 \rangle & |G_3| &= 6.6 \times 10^{5} \\
G_4 &= \langle 1 \rangle & |G_4| &= 1
\end{aligned}$$

G_{i+1} is a subgroup of G_i, and thus has cosets in G_i.

Nested Subgroups of the Rubik's Cube Group

The Rubik's Cube group G may be split into these subgroups:

$$
\begin{aligned}
G_0 &= \langle L, R, F, B, U, D \rangle & |G_0| &= 4.3 \times 10^{19} \\
G_1 &= \langle L, R, F, B, U^2, D^2 \rangle & |G_1| &= 2.1 \times 10^{16} \\
G_2 &= \langle L, R, F^2, B^2, U^2, D^2 \rangle & |G_2| &= 1.9 \times 10^{10} \\
G_3 &= \langle L^2, R^2, F^2, B^2, U^2, D^2 \rangle & |G_3| &= 6.6 \times 10^{5} \\
G_4 &= \langle 1 \rangle & |G_4| &= 1
\end{aligned}
$$

G_{i+1} is a subgroup of G_i, and thus has cosets in G_i.

Definition (Coset Space)

The set of all right cosets of H in G is called its right coset space, and is denoted $H \setminus G$.

Thistlethwaite's Algorithm

$$G_4 \leqslant G_3 \leqslant G_2 \leqslant G_1 \leqslant G_0$$

Thistlethwaite's Algorithm

$$G_4 \leqslant G_3 \leqslant G_2 \leqslant G_1 \leqslant G_0$$

Strategy: Traverse cosets in $G_{i+1} \setminus G_i$ to reach G_{i+1}. Repeat until G_4 reached.

Thistlethwaite's Algorithm

$$G_4 \leqslant G_3 \leqslant G_2 \leqslant G_1 \leqslant G_0$$

Strategy: Traverse cosets in $G_{i+1} \setminus G_i$ to reach G_{i+1}. Repeat until G_4 reached.

- From G_0 to G_1, we traverse a coset space of cardinality 2048, using all legal moves. Goal is to *orient* all the edges.

Thistlethwaite's Algorithm

$$G_4 \leqslant G_3 \leqslant G_2 \leqslant G_1 \leqslant G_0$$

Strategy: Traverse cosets in $G_{i+1} \setminus G_i$ to reach G_{i+1}. Repeat until G_4 reached.

- From G_0 to G_1, we traverse a coset space of cardinality 2048, using all legal moves. Goal is to *orient* all the edges.
- $|G_2 \setminus G_1| = 1082565$. Goal is to orient all the corners.

Thistlethwaite's Algorithm

$$G_4 \leqslant G_3 \leqslant G_2 \leqslant G_1 \leqslant G_0$$

Strategy: Traverse cosets in $G_{i+1} \setminus G_i$ to reach G_{i+1}. Repeat until G_4 reached.

- From G_0 to G_1, we traverse a coset space of cardinality 2048, using all legal moves. Goal is to *orient* all the edges.
- $|G_2 \setminus G_1| = 1082565$. Goal is to orient all the corners.
- $|G_3 \setminus G_2| = 29400$. Goal is to correctly position the corners (which may lose orientation here), and put edges in their correct *slices*.

Thistlethwaite's Algorithm

$$G_4 \leqslant G_3 \leqslant G_2 \leqslant G_1 \leqslant G_0$$

Strategy: Traverse cosets in $G_{i+1} \setminus G_i$ to reach G_{i+1}. Repeat until G_4 reached.

- From G_0 to G_1, we traverse a coset space of cardinality 2048, using all legal moves. Goal is to *orient* all the edges.
- $|G_2 \setminus G_1| = 1082565$. Goal is to orient all the corners.
- $|G_3 \setminus G_2| = 29400$. Goal is to correctly position the corners (which may lose orientation here), and put edges in their correct *slices*.
- $|G_4 \setminus G_3| = 663,552$. Goal is to re-orient the corners and position the edges, solving the cube.

Thistlethwaite's Algorithm

$$G_4 \leqslant G_3 \leqslant G_2 \leqslant G_1 \leqslant G_0$$

Strategy: Traverse cosets in $G_{i+1} \setminus G_i$ to reach G_{i+1}. Repeat until G_4 reached.

- From G_0 to G_1, we traverse a coset space of cardinality 2048, using all legal moves. Goal is to *orient* all the edges.
- $|G_2 \setminus G_1| = 1082565$. Goal is to orient all the corners.
- $|G_3 \setminus G_2| = 29400$. Goal is to correctly position the corners (which may lose orientation here), and put edges in their correct *slices*.
- $|G_4 \setminus G_3| = 663,552$. Goal is to re-orient the corners and position the edges, solving the cube.

Move choices are done using look-up tables.

That's All, Folks!

Thank you :)

That's All, Folks!

Thank you :)

(Sources will be sent later)

That's All, Folks!

Thank you :)

(Sources will be sent later)

Questions? Comments? Concerns?

qr codes or something idk