

Sims' Algorithm and Rubik's Cube

Peter Brooksbank

Department of Mathematics

The Ohio State University

Columbus, OH 43210

`brooksbank@math.ohio-state.edu`

`www.math.ohio-state.edu/~brooksbank`

Overview

- What Groups **ARE** and what Groups **WERE**
- Groups and Puzzles
- Groups and Computers
- Solving Rubik's Cube

What Groups ARE

These days, we typically think of groups in an abstract, axiomatic manner:

A **group** is a pair (G, \star) satisfying:

(G1) $x, y \in G$ implies $x \star y \in G$.

(G2) If $x, y, z \in G$, then $x \star (y \star z) = (x \star y) \star z$.

(G3) There exists an **identity** element $e \in G$ such that $x \star e = e \star x = x$ for all $x \in G$.

(G4) Every element $x \in G$ has an **inverse** $x^{-1} \in G$ such that $x \star x^{-1} = x^{-1} \star x = e$.

What Groups WERE

Historically, groups were studied in more concrete settings. For example, as groups of

- symmetries
- permutations
- transformations

Permutation Groups

$[1, n] = \{1, 2, \dots, n\}$, n an integer

$S_n = \{ \text{all bijections } \sigma : [1, n] \rightarrow [1, n] \}$

FACT : (S_n, \circ) is a group. (\circ is function composition)

A **permutation group** is a subgroup of S_n for some n .

Elements of S_n are usually written in **permutation notation**:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in S_5$$

The 15 Puzzle

Can the puzzle on the right be solved?

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

5	7	13	14
1		15	9
11	2	4	10
12	8	3	6

Each legal move is a **transposition** involving the blank square.

The solution may be regarded as the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & B \\ 5 & 7 & 13 & 14 & 1 & B & 15 & 9 & 11 & 2 & 10 & 4 & 12 & 8 & 3 & 6 \end{pmatrix}$$

A Simple Test

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

5	7	13	14
1		15	9
11	2	4	10
12	8	3	6

Write the permutation as a **product** of transpositions:

$$(1\ 5) \circ (11\ 10) \circ (9\ 11) \circ (8\ 9) \circ (14\ 8) \circ (4\ 14) \circ \\ (12\ 4) \circ (13\ 12) \circ (3\ 13) \circ (15\ 3) \circ (7\ 15) \circ (2\ 7) \circ (6\ 12)$$

There are **13** transpositions in this expression. It follows that **ANY** product of transpositions representing our permutation must contain an **odd** number of terms.

But any solution of the puzzle has an **even** number of moves!

(Can you see why?)

Rubik's Cube



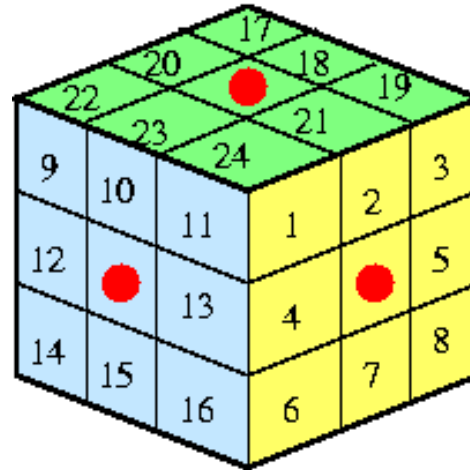
Genius!



The Hidden Truth...



The Cube as a Permutation Group



Corresponding to each 90 degree rotation of a face, there is a permutation of the numbers $\{1, \dots, 48\}$. These 6 basic *twists* generate the *cube group* \mathcal{C} .

		5	6				
		7	8				
1	2	9	10	13	14	17	18
3	4	11	12	15	16	19	20
		21	22				
		23	24				

The minicube group, \mathcal{M} , is generated by the permutations

$$\sigma_1 = (1\ 2\ 4\ 3) \circ (9\ 21\ 20\ 5) \circ (11\ 23\ 18\ 7)$$

$$\sigma_2 = (5\ 6\ 8\ 7) \circ (17\ 13\ 9\ 1) \circ (18\ 14\ 10\ 2)$$

$$\sigma_3 = (9\ 10\ 12\ 11) \circ (7\ 13\ 22\ 4) \circ (21\ 2\ 8\ 15)$$

$$\sigma_4 = (21\ 22\ 24\ 23) \circ (3\ 11\ 15\ 19) \circ (4\ 12\ 16\ 20)$$

$$\sigma_5 = (13\ 14\ 16\ 15) \circ (10\ 6\ 19\ 22) \circ (12\ 8\ 17\ 24)$$

$$\sigma_6 = (17\ 18\ 20\ 19) \circ (6\ 1\ 23\ 10) \circ (5\ 3\ 24\ 14)$$

\mathcal{C} = the cube group
 \vee
 \mathcal{C}_1 = subgroup of \mathcal{C} fixing the top corners
 \vee
 \mathcal{C}_2 = subgroup of \mathcal{C}_1 fixing 3 top edges
 \vee
 \mathcal{C}_3 = subgroup of \mathcal{C}_2 fixing the bottom corners
 \vee
 \mathcal{C}_4 = subgroup of \mathcal{C}_3 fixing the bottom edges
 \vee
 \mathcal{C}_5 = subgroup of \mathcal{C}_4 fixing the last top edge
 \vee
 $\{ () \}$ = the solved cube

Some standard algorithmic permutation group problems:

Suppose a group G is given via a generating set $X \subseteq S_n$

1. Find $|G|$.
2. Given $\sigma \in S_n$, test whether $\sigma \in G$.
3. Given $\sigma \in G$, write σ as a word in X .

How do these problems translate into cube language?

(where, for example, $G = \mathcal{C} = \langle \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6 \rangle$)

1. How many **legitimate** configurations are there?
2. Given an **arbitrary** configuration of the cube, decide whether or not the puzzle can be solved.
3. Given a **legitimate** configuration of the cube, find a sequence of twists that solves it.

Sims' Algorithm

Algorithms for permutation groups make use of a general construction known as a **point-stabilizer chain**.

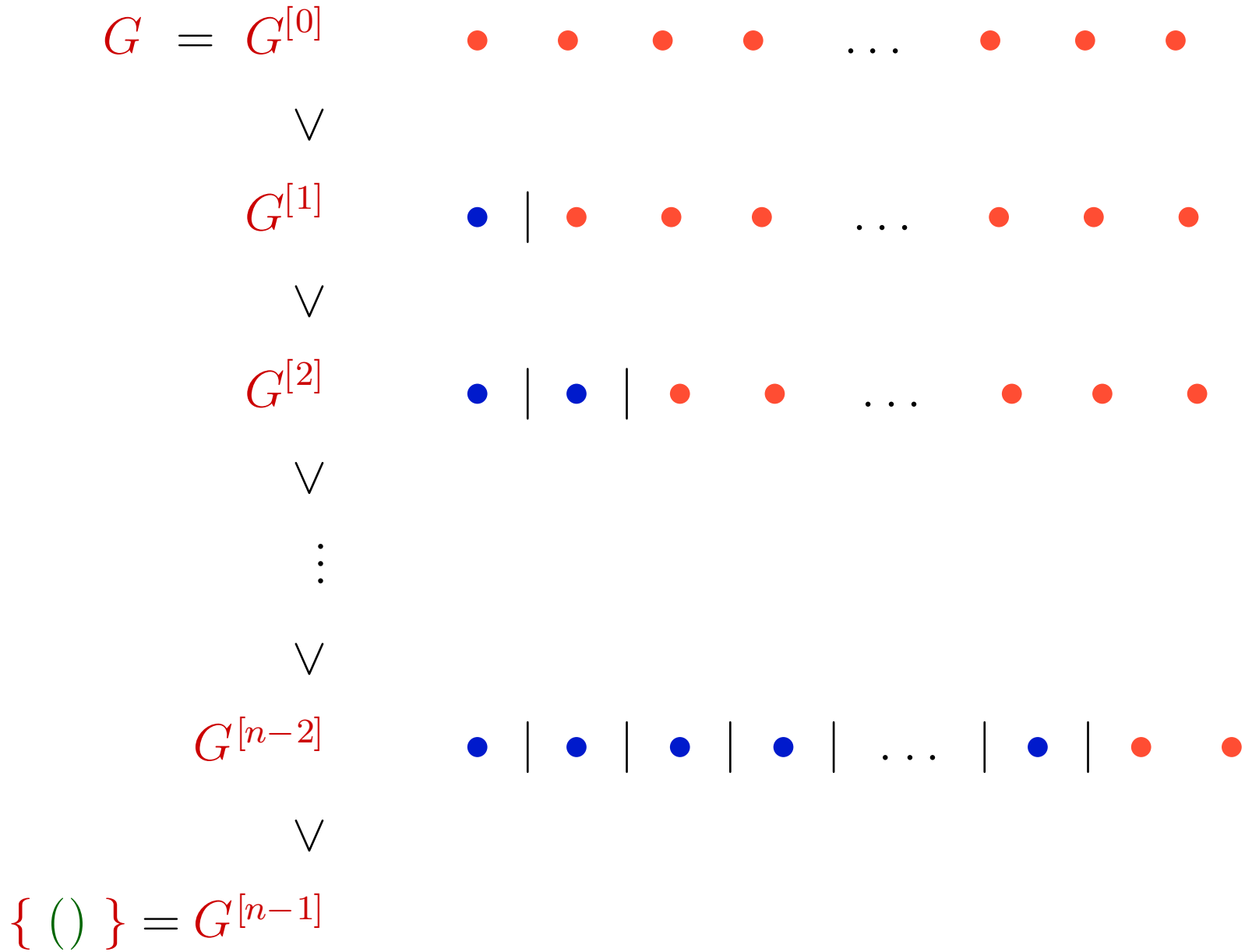
Sims' algorithm is a procedure for constructing this chain.

Having a point-stabilizer chain for a given group enables us to solve the three problems we have just been discussing, and therefore provides insight into how a computer might try to solve the cube.

A **point-stabilizer subgroup** of a group $G \leq S_n$ is defined as follows:

$$G_1 = \{ \sigma \in G \mid 1^\sigma = 1 \}$$

Point-Stabilizer Chain



Computing with \mathcal{C} using GAP

Using the 6 generator input for \mathcal{C} :

1. GAP computed the point-stabilizer chain in one tenth of a second; the order

$$|\mathcal{C}| = 43,252,003,274,489,856,000$$

came free with the construction.

2. Testing membership in \mathcal{C} of an arbitrary $\sigma \in S_{48}$ takes GAP essentially no time at all, once a stabilizer-chain has been found.

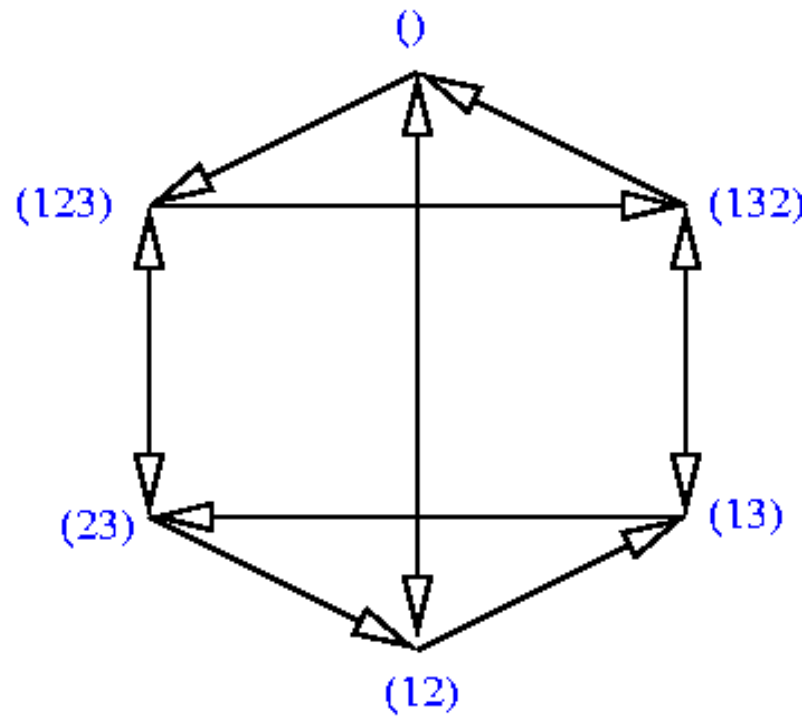
GAP doesn't do so well in providing useful solutions for the cube:

- Solutions typically require 1200 twists.
- Speed cubers use, on average, 60 twists.

Some Other Cube Related Problems

- Given some legitimate configuration of a cube puzzle, what is the **minimum** number of twists required to solve it?
- What is the **smallest** number, N , such that **ANY** legitimate configuration of a cube puzzle can be solved using at most N twists?

$$\Gamma(S_3 , \{ (1\ 2) , (1\ 2\ 3) \})$$



Some Answers

- For the minicube, the answer is known:

$$\Delta(\mathcal{M}, \{\sigma_1^{\pm 1}, \dots, \sigma_6^{\pm 1}\}) = 11.$$

This was demonstrated by [Gene Cooperman](#).

- For the regular cube, it is known that

$$\Delta(\mathcal{C}, \{\sigma_1^{\pm 1}, \dots, \sigma_6^{\pm 1}\}) \geq 24,$$

since the “[superflip](#)” configuration requires this many twists.

This was demonstrated by [Jerry Bryan](#) / [Michael Reid](#).

- It is also known that

$$\Delta(\mathcal{C}, \{\sigma_1^{\pm 1}, \dots, \sigma_6^{\pm 1}\}) \leq 42.$$

This was shown by [Michael Reid](#).

$$|C| = 43,252,003,274,489,856,000$$

“Ideal Toy Company stated on the package of the original Rubik cube that there were more than **three billion** possible states the cube could attain.

It’s analogous to McDonald’s proudly announcing that they’ve sold more than 120 hamburgers.”

J. A. Paulos, **Innumeracy**