Lecture 1.2: Cayley graphs

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

A road map for the Rubik's Cube

There are many solution techniques for the Rubik's Cube. If you do a Google search, you'll find several methods for solving the puzzle.

These methods describe a sequence of moves to apply relative to some starting position. In many situations, there may be a shorter sequence of moves that would get you to the solution.

In fact, it was shown in July 2010 that every configuration is at most 20 moves away from the solved position!

Let's pretend for a moment that we were interested in writing a complete solutions manual for the Rubik's Cube.

Let me be more specific about what I mean.

A road map for the Rubik's Cube

We'd like our solutions manual to have the following properties:

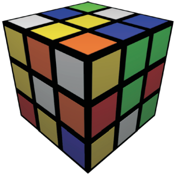
1. Given any scrambled configuration of the cube, there is a unique page in the manual corresponding to that configuration.
2. There is a method for looking up any particular configuration. (The details of how to do this are unimportant.)
3. Along with each configuration, a list of available moves is included. In each case, the page number for the outcome of each move is included, along with information about whether the corresponding move takes us closer to or farther from the solution.

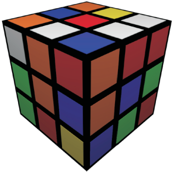
Let's call our solutions manual the *Big Book*.

Page 12,574,839,257,438,957,431 from the *Big Book*

You are **15 steps** from the solution.

Cube front





Cube back

Face	**Direction**	**Destination page**	**Progress**
Front	Clockwise	36,131,793,510,312,058,964	Closer to solved
Front	Counterclockwise	12,374,790,983,135,543,959	Farther to solved
Back	Clockwise	26,852,265,690,987,257,727	Closer to solved
Back	Counterclockwise	41,528,397,002,624,663,056	Farther to solved
Left	Clockwise	6,250,961,334,888,779,935	Closer to solved
Left	Counterclockwise	10,986,196,967,552,472,974	Farther to solved
Right	Clockwise	26,342,598,151,967,155,423	Farther to solved
Right	Counterclockwise	40,126,637,877,673,696,987	Closer to solved
Top	Clockwise	35,131,793,510,312,058,964	Closer to solved
Top	Counterclockwise	33,478,478,689,143,786,858	Farther to solved
Bottom	Clockwise	20,625,256,145,628,342,363	Farther to solved
Bottom	Counterclockwise	7,978,947,168,773,308,005	Closer to solved

A road map for the Rubik's Cube

We can think of the *Big Book* as a road map for the Rubik's Cube. Each page says, "you are here" and "if you follow this road, you'll end up over there."

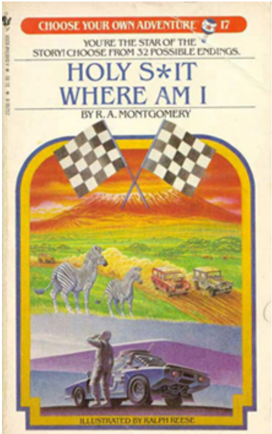


Figure: Potential cover and alternative title for the *Big Book*

A road map for the Rubik's Cube

Unlike a vintage *Choose Your Own Adventure* book, you'll additionally know whether "over there" is where you want to go or not.

Pros of the *Big Book*:

- We can solve any scrambled Rubik's Cube.
- Given any configuration, every possible sequence of moves for solving the cube is listed in the book (long sequences and short sequences).
- The *Big Book* contains complete data on the moves in the Rubik's Cube universe and how they combine.

Cons of the *Big Book*:

- We just took all the fun out of the Rubik's Cube.
- If we had such a book, using it would be fairly cumbersome.
- We can't actually make such a book. Rubik's Cube has more than 4.3×10^{19} configurations. The paper required to write the book would cover the Earth many times over. The book would require over a billion terabytes of data to store electronically, and no computer in existence can store that much data.

What have we learned?

Despite the *Big Book*'s apparent shortcomings, it made for a good thought experiment.

The most important thing to get out of this discussion is that the *Big Book* is a map of a group.

We shall not abandon the mapmaking ideas introduced by our discussion of the *Big Book* simply because the map is too large.

We can use the same ideas to map out any group. In fact, we shall frequently do exactly that.

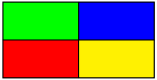
Let's try something simpler. . .

The Rectangle Puzzle

- Consider a clear glass **rectangle** and label it as follows:

1	2
4	3

If you prefer, you can use colors instead of numbers:



We'll use numbers, and call the above configuration the **solved state** of our puzzle.

- The idea of the game is to scramble the puzzle and then find a way to return the rectangle to its solved state.

- We are allowed two moves: horizontal flip and vertical flip, where "horizontal" and "vertical" refer to the motion of your hands, rather than any reference to an axis of reflection.

  Loosely speaking, we only allow these moves because they preserve the "footprint" of the rectangle. Do any other moves preserve its footprint?

The Rectangle Puzzle

Question

Do the moves of the Rectangle Puzzle form a group? How can we check?

For reference, here are the rules of a group:

Rule 1

There is a predefined list of actions that never changes.

Rule 2

Every action is reversible.

Rule 3

Every action is deterministic.

Rule 4

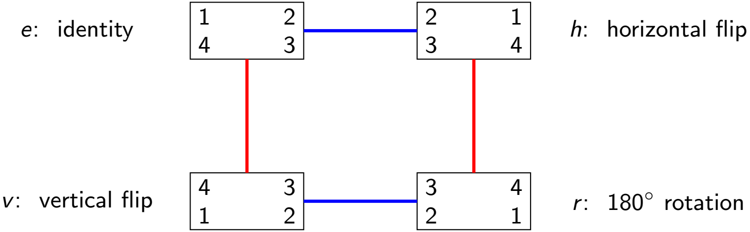
Any sequence of consecutive actions is also an action.

Road map for The Rectangle Puzzle

For our covenience, let's say that when we flip the rectangle, the numbers automatically become "right-side-up," as they would if you rotated an iPhone.

It is not hard to see that using only sequences of horizontal and vertical flips, we can obtain only four configurations.

Unlike the Rubik's cube group, the "road map" of the rectangle puzzle is small enough that we can draw it.



Observations? What sorts of things does the map tell us about the group?

Observations

Let G denote the rectangle group. This is a **set** of four actions. We see:

- G has 4 actions: the "*identity*" action e, a horizontal flip h, a vertical flip v, and a 180° rotation r.

$$G = \{e, h, v, r\}.$$

- We need two actions to "generate" G. In our diagram, each **generator** is represented by a different type (color) of arrow. We write:

$$G = \langle h, v \rangle.$$

- The map shows us how to get from any one configuration to any other. There is more than one way to follow the arrows! For example

$$r = hv = vh.$$

- For this particular group, the order of the actions is irrelevant! We call such a group **abelian**. Note that the Rubik's cube group is *not* abelian.

- Every action in G is its own **inverse**: That is,

$$e = e^2 = h^2 = v^2 = r^2.$$

  The Rubik's cube group does **not** have this property. Algebraically, we write:

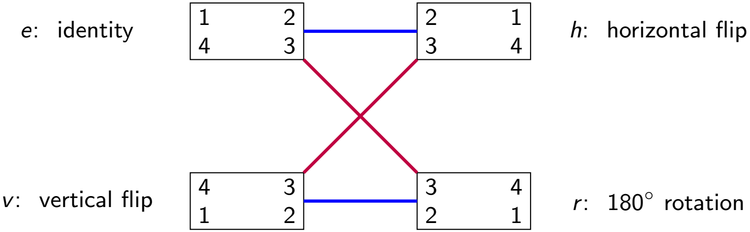
$$e^{-1} = e, \qquad v^{-1} = v, \qquad h^{-1} = h, \qquad r^{-1} = r.$$

An alternative set of generators for the Retangle Puzzle

The rectangle puzzle can also generated by a horizontal flip and a 180° rotation:

$$G = \langle h, r \rangle \, .$$

Let's build a Cayley graph using this alternative set of generators.



Do you see this road map has the "same structure" as our first one? Of course, we need to "untangle it" first.

Perhaps surprisingly, this might *not* always be the case.

That is, there are (more complicated) groups for which different generating sets yield road maps that are structurally different. We'll see examples of this shortly.

Cayley diagrams

As we saw in the previous example, how we choose to layout our map is irrelevant.

What is important is that the connections between the various states are preserved.

However, we will attempt to construct our maps in a pleasing to the eye and symmetrical way.

The official name of the type of group road map that we have just created is a Cayley diagram, named after 19th century British mathematician Arthur Cayley.

In general, a Cayley diagram consists of nodes that are connected by colored (or labeled) arrows, where:

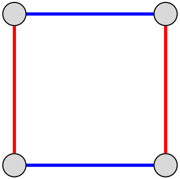
- an arrow of a particular color represents a specific generator;
- each action of the group is represented by a unique node (sometimes we will label nodes by the corresponding action).
- Equivalently, each action is represented by a (non-unique) path starting from the **solved state**.

More on arrows

- An arrow corresponding to the generator g from node x to node y means that node y is the result of applying the action $g \in G$ to node x:

- If an action $h \in G$ is its own inverse (that is, $h^2 = e$), then we have a 2-way arrow. This happens with horizontal and vertical flips. For clarity, our convention is to drop the tips on all 2-way arrows. Thus, these are exactly the same:

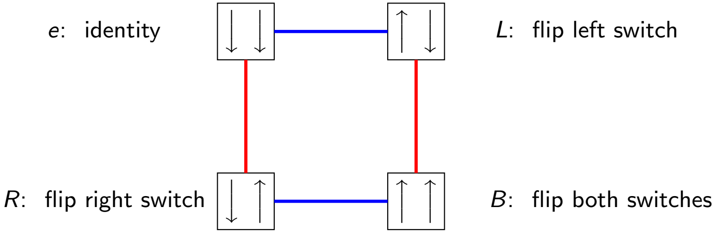
When we want to focus on a group's structure, we frequently omit the labels at the nodes. Thus, the Cayley diagram of the rectangle puzzle can be drawn as follows:



The 2-Light Switch Group

Let's map out another group, which we'll call the *2-Light Switch Group*:

- Consider two light switches side by side that both start in the off position (This is our "solved state").
- We are allowed 2 actions: flip L switch and flip R switch.



Notice how the Cayley diagrams for the Rectangle Puzzle $G = \{e, v, h, r\}$ and the 2-Light Switch Group $G' = \{e, L, R, B\}$ are essentially the same.

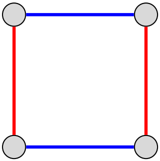
Although these groups are superficially different, the Cayley diagrams help us see that *they have the same structure*. (The fancy phrase for this property is that the "*two groups are isomorphic*"; more on this later.)

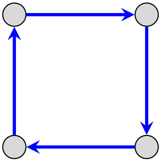
The Klein 4-group

Any group with the same Cayley diagram as the Rectangle Puzzle and the 2-Light Switch Group is called the Klein 4-group, denoted by V_4 for *vierergruppe*, "four-group" in German. It is named after the mathematician Felix Klein.

It is important to point out that the number of different types (i.e., colors) of arrows matters. For example, the Cayley diagram on the right *does not* represent V_4.

$G = V_4$





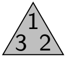
$G = ???$

Questions

- What group has a Cayley graph like the diagram on the right?
- How would you give a proof (=convincing argument) that these two groups have truly different structures? Can you find a property that one group has that the other does not?
- Can you find another group of size 4 that is different from both of these?

The triangle puzzle

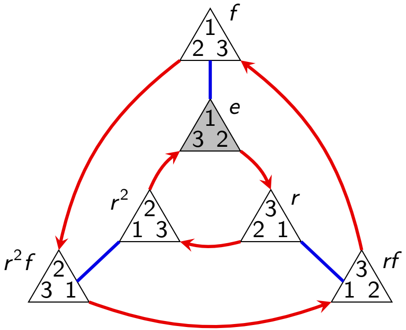
Let's play our "rectangle puzzle" game but with an equilateral triangle:



The "triangle puzzle" group, often denoted D_3, has 6 actions:

- The identity action: e
- A (clockwise) 120° rotation: r
- A (clockwise) 240° rotation: r^2
- A horizontal flip: f
- Rotate + horizontal flip: rf
- Rotate twice + horizontal flip: r^2f.

One set of generators: $D_3 = \langle r, f \rangle$.



Notice that multiple paths can lead us to the same node. These give us **relations** in our group. For example:

$$r^3 = e, \qquad r^{-1} = r^2, \qquad f^{-1} = f, \qquad rf = fr^2, \qquad r^2f = fr.$$

This group is **non-abelian**: $rf \neq fr$.

Properties of Cayley graphs

Observe that at every node of a Cayley graph, there is exactly one out-going edge of each color.

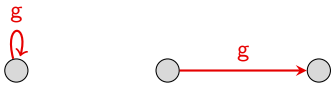
Question 1

Can an edge in a Cayley graph ever connect a node to itself?

Question 2

Suppose we have an edge corresponding to generator g that connects a node x to itself. Does that mean that the edge g connects *every* node to itself? In other words, can an action be the *identity action* when applied to some actions (or configurations) but not to others?

Visually, we're asking if the following scenerio can ever occur in a Cayley diagram:



A Theorem and Proof!

Perhaps surprisingly, the previous situation is *impossible*! Let's properly formulate and prove this.

Theorem

Suppose an action g has the property that $gx = x$ for some other action x. Then g is the *identity action*, i.e., $gh = h = hg$ for all other actions h.

Proof

The identity action (we'll denote by 1) is simply the action hh^{-1}, for any action h.

If $gx = x$, then multipling by x^{-1} *on the right* yields:

$$g = gxx^{-1} = xx^{-1} = 1.$$

Thus g is the identity action. □

This was our first mathematical proof! It shows how we can deduce interesting properties about groups *from* the rules, which were not explicitly *built into* the rules.