## CS64: Computation for Puzzles and Games



Autumn 2022
Lecture 8: The 15-Puzzle and Rubik's Cube

## Announcements

- No in-person puzzle session this Friday, since everyone is probably heading off for break anyway...
- But I may post some on Canvas!
- This is the final week to withdraw, but there is little incentive to do so.
- This week I'll send a form where you can let me know if you have attended / will attend enough of the lectures, or plan to do a small project.
- More info on the class puzzle hunt coming soon! I'm excited!


## Al world domination update

## ars TECHNICA

New Go-playing trick defeats world-class Go AI-but loses to human amateurs

An adversarial strategy tricks KataGo (which is kinda like AlphaZero) into ending the game early because it thinks it's so far ahead

Adversarial policy attacks blind spots in the AI-with broader implications than games.



## Two crazes, a century apart


a mania in 1880

a fad in the 1980 s

## The 15-Puzzle



\section*{| 1 | 3 |
| :--- | :--- |
| 5 | 7 |
| 9 | 11 |
| 13 | 15 |}

Perhaps the quintessential stock
 public-domain puzzle. Shows up all over the place in games etc.

## A national mania in early 1880

The reports come in slowly. Only one man went crazy over the Fifteen Block Puzzle yesterday, and he was a Pennsylvanian.

From a Cincinnati paper. Apologies to any Pennsylvanians in the class!


But why was this puzzle thought of as so exasperating and complicated?

## They were doing it wrong

The comic whekly Puck has an amusing cartoon representing Conkling in a state of desperation over the "Fifteen" puzzle. Each block has the face of some Presidential candidate, Grant, Blaine $\boldsymbol{q}^{\text {monern }}$ esenting the mystic thre , 13, 15, 14. Do what he will, Conkliry camou bet Grant in the right place, Blaine or Tilden invariably coming out first at the end. Some one sent a conv of the nomar ta b

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

## They were doing it wrong

THE Comic weekly Pack has an amusing cartoon representing Conkling in a state of desperation over the "Fifteen" puzzle. Each block has the face of some Presidential candidate,
 the mystic thre, $13,15,14$. Do what he will, Conklimg eammo ber Grant in the right place, Blaine or Tilden in- " variably coming out first at the end. " Soine one sent a eonv of the nomar in b

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

## They were doing it wrong

The comic wrekly $\boldsymbol{P}_{\text {ded }}$ has an amusing cartoon representing Conkling in a state of desperation over the "Fifteen" puzzle. Each block has the fince of some Presidential candidate,
 the mystic thre , 13, 15, 14. Do what he will, Conklimg eamourer Grant in the right place, Blaine or Tilden in- " variably coming out first at the end. " Some one sent a eonv of the nonary tal b

| 1 | 2 | 3 | 4 |
| :---: | :---: | :---: | :---: |
| 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 |
| 13 | 15 | 14 |  | remaining. The blocks are all given a

number from one to ifteen inclusive, and
are put into the box at random. The
numala coneiata in cettiner them in con-

It turns out that only half of all starting configurations are solvable!

Aside: old newspaper ads are fun

## CELERY

As a Remedy for Nervous Diseases.

What the Medical Profession Say About It,


The Cood Results Attending Its Use

Headache, Neuralgia, Nervousness, Indigestion, Sleeplessness and Paralysis,

Aside: old newspaper ads are fun

## CELERY


 seveatics I drove the entire world crazy over a little box of movalle Whocks which became known as the "14-15 Puzzle" The fifteen blocks
regular order, only with the 14 and 15 reversel, as shown in the above illustration. The puzzle consisted in moving the blocks about, one at a time, so as to bring them back a the present position in every respect

A prize of $\$ 1,000$, which was of fered for the first correct solution to be problem, has never been claimed, othough there are thousands of pertons who say they periormed the reguired fat.
he went for his noon lunch and was discovered by his frantic staff long past midnight pushing little pieces of pic around on a plate! Farmers are known to have deserted their plows and I have taken one of such instances as an illustration for the ketch.
Several new problems developed from the original puzzle which are worth giving.
Second Problem-Start again with the blocks as in Fig. 1 and move them so as to get the numbers in regular orcer, but with the vacant square at upper left-hand corner instead of ower right-hand corner ; see Fig. 2. Third Problem-Start with Fig , turn the box a quarter way round and so move the blocks that they
vill rest as in Fig. 3
Fourth Problem-This is to move



The Picnic Puzzle.
When they started off on the great annu: 1 picnic every wagon in town wav pressed into service. Half way to the grounds ten wagons broke down, so it was necessary for each of the remaining wagons to carry one more person.
When they started for home it was discovered that fifteen more wagons were out of commission, so on the return trip there were three persons more in each wagon than

Writing decades after the fact, Sam Loyd falsely claimed to have invented the 15-puzzle.

> He also offered a \$1000 prize (closer to \$30000 today?) for solving this impossible variant...

## One easy(ish) check for solvability

- Start with a 1 if the empty cell is in the top or third row, or a 0 if the empty cell is in the second or bottom row.
- Then count the number of pairwise inversions in the order of the pieces, reading left-to-right, then top to bottom. Take 1 if this number is odd, or 0 if it's even.
- The puzzle is solvable if and only if the sum of these is even.


## One easy(ish) check for solvability

- Start with a 1 if the empty cell is in the top or third row, or a 0 if the empty cell is in the second or bottom row.
- Then count the number of pairwise inversions in the order of the pieces, reading left-to-right, then top to bottom. Take 1 if this number is odd, or 0 if it's even.
- The puzzle is solvable if and only if the sum of these is even.


## One easy(ish) check for solvability

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

- Then count the number of pairwise inversions in the order of the pieces, reading left-to-right, then top to bottom. Take 1 if this number is odd, or 0 if it's

Empty cell position: Third even.

- The puzzle is solvable if and only if the sum of these is even.


## One easy(ish) check for solvability



- Then count the number of pairwise inversions in the order of the pieces, reading left-to-right, then top to bottom. Take 1 if this number is odd, or 0 if it's even.
- The puzzle is solvable if and only if the sum of these is even.

Empty cell position: Third row = 1

Inversions: 6-5, 6-4, 5-4, 13-12, 14-12, 15-12
6 total = 0

## One easy(ish) check for solvability

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

- Then count the number of pairwise inversions in the order of the pieces, reading left-to-right, then top to bottom. Take 1 if this number is odd, or 0 if it's even.
- The puzzle is solvable if and only if the sum of these is even.

Empty cell position: Third row = 1

Inversions: 6-5, 6-4, 5-4, 13-12, 14-12, 15-12
6 total $=$ even $=0$
$1+o=1$. Not even, so not solvable!

## Why does this work?

- If we move a piece within a row:
- The row number of the blank cell doesn't change.
- No inversions are created or destroyed.
- Therefore, no change in our metric.

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

## Why does this work?

- If we move a piece within a row:
- The row number of the blank cell doesn't change.
- No inversions are created or destroyed.
- Therefore, no change in our metric.

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

- If we move a piece within a column:
- The row number of the blank cell changes by $\pm 1$, so we go from a 0 to a 1 or vice versa.


## Why does this work?

- If we move a piece within a row:
- The row number of the blank cell doesn't change.
- No inversions are created or destroyed.
- Therefore, no change in our metric.

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

- If we move a piece within a column:
- The row number of the blank cell changes by $\pm 1$, so we go from a 0 to a 1 or vice versa.
- The number of inversions changes by $\pm 1$ or $\pm 3$.


## Why does this work?

- If we move a piece within a row:
- The row number of the blank cell doesn't change.
- No inversions are created or destroyed.
- Therefore, no change in our metric.

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

- If we move a piece within a column:
- The row number of the blank cell changes by $\pm 1$, so we go from a 0 to a 1 or vice versa.
- The number of inversions changes by $\pm 1$ or $\pm 3$.
- The piece is moving to the other side of a block of 3 cells, and nothing else is changing.
- If it had inversions with $0,1,2$, or 3 of them, it now has inversions with $3,2,1$, or 0 , respectively, for a net change of $-3,-1,+1$, or +3 .


## Why does this work?

- If we move a piece within a row:
- The row number of the blank cell doesn't change.
- No inversions are created or destroyed.
- Therefore, no change in our metric.

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

- If we move a piece within a column:
- The row number of the blank cell changes by $\pm 1$, so we go from a 0 to a 1 or vice versa.
- The number of inversions changes by $\pm 1$ or $\pm 3$.
- The piece is moving to the other side of a block of 3 cells, and nothing else is changing.
- If it had inversions with $0,1,2$, or 3 of them, it now has inversions with $3,2,1$, or 0 , respectively, for a net change of $-3,-1,+1$, or +3 .
- Our metric doesn't change (odd + odd = even)


## Why does this work?

- If we move a piece within a row:
- The row number of the blank cell doesn't change.
- No inversions are created or destroyed.
- Therefore, no change in our metric.

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

- If we move a piece within a column:
- The row number of the blank cell changes by $\pm 1$, so we go from a 0 to a 1 or vice versa.
- The number of inversions changes by $\pm 1$ or $\pm 3$.
- The piece is moving to the other side of a block of 3 cells, and nothing else is changing.
- If it had inversions with $0,1,2$, or 3 of them, it now has inversions with $3,2,1$, or 0 , respectively, for a net change of $-3,-1,+1$, or +3 .
- Our metric doesn't change (odd + odd = even)
- Since the final state has no inversions and its empty cell in the bottom right, the metric is even there. And valid moves don't change that!


## Didn't they know this in 1880 ?

- Yes! Even in 1879!
©
JOURNAL ARTICLE OPEN ACCESS
Notes on the "15" Puzzle
Wm. Woolsey Johnson and William E.
Story

| American Joural. <br> of Matamatics |
| :--- | | American Journal of |
| :--- |
| Mathematics |
| Vol. 2, No. 4 (Dec., |

1879), pp. 397-404 (8
pages)

It seems to be generally supposed, by those who have tried the puzzle, that this is always possible, whatever be the original random position of the counters, but this is an error, as the following demonstration will show :

When the blank or sixteenth square is the vacant one, the arrangement of the counters may be called a positive or negative one, according as the term of the 15 -square determinant, which has for first and second subscripts

## Didn't they know this in 1880 ?

- Yes! Even in 1879!
- But imagine trying to explain this in the newspaper. Most people probably wouldn't have been receptive to arguments based on parity and/or permutations.
- Even today!


## What Is the Answer to That Stupid Math Problem on Facebook?

And why are people so riled up about it?

BY TARA HAELLE


## Didn't they know this in 1880 ?

- Yes! Even in 1879!
- But imagine trying to explain this in the newspaper. Most people probably wouldn't have been receptive to arguments based on parity and/or permutations.
- Even today!
- The puzzle offers so much superficial freedom to explore, so it is hard to convince someone that none of that matters.
- Depending on the manufacturing quality, it might have been all too easy to make an accidental illegal move somewhere, then think you'd solved an impossible puzzle.
- Solutions are long, so probably no one was writing them down as they went


## A callout $140+$ years later

| Wrong! | Joseph W. Meyers, Esq., Captain of our Police Force, is the only man in Ohio wh claims to be able to work out the "fifteen" |
| :---: | :---: |
|  | in any shape. He can do it |
|  | on a wager rrom one to seven hundred and does it with his mittens on, blindfolded or wit his hands tied behind him-in his mind. |

My take: the newspaper column writer is having a bit of fun and setting up annoyance for his friend

## How hard is it (for solvable states)?

- Lights Out: Fixing stuff breaks other stuff. Hard to progress toward a goal in an obvious way.
- Rubik's Cube: Solving one face of the cube is not too hard, but then fixing stuff breaks (or at least temporarily breaks) other stuff.
- 15-Puzzle: You can solve most of the grid and then fix the remaining part.


## Demo: solving by hand

- "Scoop and loop" method (I just made up this name - it's not an actual thing)


## That was inefficient - can we do better?

- Sure, we can find a shortest solution...
- What kind of starting grid do you think would be the worst (i.e., require the largest number of moves)?

The 17 positions which need 80 moves are

|  |  | 9 |  |  |  | 10 | 13 |  |  | 9 |  |  |  | 9 |  |  |  | ) 9 | 13 | 121413 |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 11 | 10 |  |  | 11 | 14 | 9 |  | 15 | 10 | 14 |  | 12 | 10 |  |  | 511 | 110 |  |  | 11 |  | 10 |
| 3 | 7 | 2 | 5 | 3 | 7 | 2 | 5 | 3 | 7 | 6 | 2 | 3 | 7 | 6 | 2 | 3 | 3 | 6 | 2 | 3 | 7 |  | 2 |
| 4 | 8 | 6 | 1 | 4 | 8 | 6 | 1 | 4 | 8 | 5 | 1 | 4 | 8 | 5 | 1 | 4 | 8 | 5 | 1 | 4 | 8 |  | 1 |
|  |  | 10 | 13 |  |  | 11 | 13 |  |  | 10 | 113 |  | 12 | 9 |  |  |  | 29 |  | 121413 |  |  |  |
|  | 11 | 14 | 9 |  | 14 | 10 | 9 |  | 11 | 9 | 14 |  | 11 |  | 10 |  | 511 | 10 | 14 | 15 | 11 |  | 10 |
| 3 | 7 | 6 | 2 | 3 | 7 | 6 | 2 | 7 | 3 | 6 | 2 | 3 | 8 | 6 | 2 | 8 | 3 | 6 | 2 | 8 | 3 | 6 | 2 |
| 4 | 8 | 5 | 1 | 4 | 8 | 5 | 1 | 4 | 8 | 5 | ) 1 | 4 | 7 | 5 | 1 | 4 | 4 | 5 | 1 | 4 | 7 |  | 1 |
|  |  | 19 |  |  |  | 1 | )13 |  |  | 9 | 13 |  |  | 9 |  |  |  | 19 |  |  |  |  |  |
|  |  | 10 | 114 | 15 | 11 | 14 | , | 15 | 8 |  | 014 |  | 11 | 10 | 14 |  | 511 |  |  |  |  |  |  |
| 7 | 8 | 6 | 2 | 7 | 8 | 6 | 2 | 11 | 7 | 6 | 2 | 3 | 7 | 5 | 6 | 7 | 78 | 5 | 6 |  |  |  |  |
| 4 | 3 | 5 | 1 | 4 | 3 | 5 | 1 | 4 | 3 | 5 | 51 | 4 | 8 | 2 | 1 | 4 | 4 | 2 | 2 |  |  |  |  |

Sort of reversed, but not exactly. (Note: a pure reverse could actually be helpful, e.g., 4-3-2-1 could be rotated to the top.)

## BFS vs. DFS

- Breadth-first search (BFS)
- finds all states 1 move away from the start state,
- then all states that are 2 moves away,
- and so on until it finds the goal state.

Plodding! Has to exhaustively try everything shorter before it finds an answer, and also remember an increasingly large band of states.

- Depth-first search (DFS)
- looks much more like a human solving the puzzle...
- but a human with an amazing memory who knows not to repeat a state, and remembers how to backtrack when they get stuck.
Risky! Can get lucky fast, or can go way off into the weeds.


## Iterative deepening

Do DFS but only up to depth 1 . Then do it again (starting over) but only down to depth 2 ... and so on until a solution is found.

First thought: isn't this worse? It does a bunch of redundant work!

## Iterative deepening

Do DFS but only up to depth 1. Then do it again (starting over) but only down to depth 2 ... and so on until a solution is found.

First thought: isn't this worse? It does a bunch of redundant work!
Second thought: well, most of the work is in the bottom layer of the tree anyway, so that's not so bad...

And this strategy uses much less memory than BFS, which has to keep track of every solution at a given depth.

It also can't miss a solution within the specified depth range, unlike DFS which could shoot past it.

## Is the 15 -puzzle NP-complete?

- Depends on what we mean!
- First of all, we have to talk about generalizations to $n \times n$ boards and study the asymptotic behavior. Any particular finite board is solvable in $\mathrm{O}(1)$ time, technically!


## Is the 15 -puzzle NP-complete?

- Depends on what we mean!
- First of all, we have to talk about generalizations to $n \times n$ boards and study the asymptotic behavior. Any particular finite board is solvable in $\mathrm{O}(1)$ time, technically!
- Even then, what problem do we mean?

■ "Can it be solved?" - this is polynomial and we saw how

## Is the 15 -puzzle NP-complete?

- Depends on what we mean!
- First of all, we have to talk about generalizations to $n \mathrm{x} n$ boards and study the asymptotic behavior. Any particular finite board is solvable in $\mathrm{O}(1)$ time, technically!
- Even then, what problem do we mean?
- "Can it be solved?" - this is polynomial and we saw how
- "Find me a series of moves that solves it" - also polynomial time


## Is the 15 -puzzle NP-complete?

- Depends on what we mean!
- First of all, we have to talk about generalizations to $n \mathrm{x} n$ boards and study the asymptotic behavior. Any particular finite board is solvable in $\mathrm{O}(1)$ time, technically!
- Even then, what problem do we mean?
- "Can it be solved?" - this is polynomial and we saw how
- "Find me a series of moves that solves it" - also polynomial time
- "Can it be solved within $k$ moves" - this is NP-complete


## The Rubik's Cube

- Invented in the 1970s, exploded onto the world stage in 1980
- Still a huge competitive scene
- until recently there was even a category for fastest solve using feet

culture. To date, over 350 million Rubik's Cubes have been sold, making it one of the best selling toys of all time. It became very famous and today, there are many sizes from $2 \times 2$ o 21x21. [7][9]


## Another game/puzzle where robots are better?



## Another game/puzzle where robots are better?



Everything Gamer 2 years ago
Imposible plot twist: the machine sprays paint in 0.38 second
$\because 3.1 \mathrm{~K}$ Reply

## Major recent results

- No configuration requires more than 20 moves (2010; Rokicki, Kociemba, Davidson, Dethridge)
- Was not just "run Google computers on every possible configuration" (there are 43 quintillion of them)
- "Can this configuration be solved in $k$ moves" is NP-complete (2017; Demaine, Eisenstadt, Rudoy)
- Reduction from the known NP-complete "is there a Hamiltonian path from $a$ to $b$ in this graph?" problem


# THE DIAMETER OF THE RUBIK'S CUBE GROUP IS TWENTY* 

TOMAS ROKICKI ${ }^{\dagger}$, HERBERT KOCIEMBA ${ }^{\ddagger}$, MORLEY DAVIDSON ${ }^{\S}$, AND JOHN DETHRIDGE ${ }^{〔}$

Abstract. We give an expository account of our computational proof that every position of The roughly $4.3 \times 10^{19}$ positions are partitioned into about two billion cosets of a specially chosen subgroup, and the count of cosets required to be treated is reduced by considering symmetry. The about one billion seconds of CPU time donated by Google. As a byproduct of determining that the diameter is 20 , we also find the exact count of cube positions at distance 15 .

# THE DIAMETER OF THE RUBIK'S CUBE GROUP IS TWENTY* 

TOMAS ROKICKI ${ }^{\dagger}$, HERBERT KOCIEMBA ${ }^{\ddagger}$, MORLEY DAVIDSON ${ }^{\S}$, AND JOHN DETHRIDGE ${ }^{\top}$

Abstract. We give an expository account of our computational proof that every position of The roughly $4.3 \times 10^{19}$ positions are partitioned into about two billion cosets of a specially chosen subgroup, and the count of cosets required to be treated is reduced by considering symmetry. The about one billion seconds of CPU time donated by Google. As a byproduct of determining that the diameter is 20 , we also find the exact count of cube positions at distance 15 .

Once narrowed down, this search used a version of iterative deepening.

## What is a group?

A set $G$ equipped with a binary operation $\cdot$, such that

- closure: for all $a, b$ in $G, a \cdot b$ is in $G$
- associativity: for all $a, b, c$ in $G,(a \cdot b) \cdot c=a \cdot(b \cdot c)$
- identity: there is an element in G - call it 1 - such that for each a in G, $1 \cdot a=a \cdot 1=a$
- inverse: for each $a$ in $G$, there exists $a^{-1}$ in $G$ such that $a \cdot a^{-1}=a^{-1} \cdot a=1$


## Example: set = integers, operation = addition

| closure: for all $a, b$ in $G, a \cdot b$ is in $G$ | integer + integer $=$ <br> integer |
| :--- | :--- |
| associativity: for all $a, b, c$ in $G,(a \cdot b) \cdot c$ <br> $=a \cdot(b \cdot c)$ | addition is already <br> known to be associative |
| identity: there is an element in $G-$ <br> call it $1-$ such that for each $a$ in $G, 1 \cdot a$ <br> $=a \cdot 1=a$ | the identity is 0 <br> (remember that the $\cdot$ is <br> addition here) |
| inverse: for each $a$ in $G$, there exists <br> $a^{-1}$ in $G$ such that $a \cdot a^{-1}=a^{-1} \cdot a=1$ | the inverse of $a$ is $-a$ |

## The Rubik's Cube Group

The set:

- Describe each possible reachable cube configuration by some list of operations that gets there from the solved state.
- Take the set of all such lists of operations.

The binary operation: Concatenation (starting from the solved state, perform the first list of operations, then the second)

- Unlike with our addition example, the group is notably not commutative: for two elements $a$ and $b, a \cdot b$ may yield a different result than $b \cdot a$
closure: for all $a, b$ in $G, a \cdot b$ is in $G$
associativity: for all $a, b, c$ in $G$, $(a \cdot b) \cdot c=a \cdot(b \cdot c)$
identity: there is an element in $\mathrm{G}-$ call it 1 - such that for each $a$ in G, $1 \cdot a$ $=a \cdot 1=a$
inverse: for each $a$ in $G$, there exists $a^{-1}$ in $G$ such that $a \cdot a^{-1}=a^{-1} \cdot a=1$
closure: for all $a, b$ in $G, a \cdot b$ is in $G$
composing two lists of moves puts us in a state that can itself be described by a list of moves
associativity: for all $a, b, c$ in $G$, $(a \cdot b) \cdot c=a \cdot(b \cdot c)$
identity: there is an element in G call it 1 - such that for each $a$ in G, $1 \cdot a$ $=a \cdot 1=a$
inverse: for each $a$ in $G$, there exists $a^{-1}$ in $G$ such that $a \cdot a^{-1}=a^{-1} \cdot a=1$
closure: for all $a, b$ in $G, a \cdot b$ is in $G$
associativity: for all $a, b, c$ in $G$, $(a \cdot b) \cdot c=a \cdot(b \cdot c)$
composing two lists of moves puts us in a state that can itself be described by a list of moves
in both cases the combined ordered list of moves is the same
identity: there is an element in $\mathrm{G}-$ call it 1 - such that for each $a$ in G, $1 \cdot a$ $=a \cdot 1=a$
inverse: for each $a$ in $G$, there exists $a^{-1}$ in $G$ such that $a \cdot a^{-1}=a^{-1} \cdot a=1$
closure: for all $a, b$ in $G, a \cdot b$ is in $G$
associativity: for all $a, b, c$ in $G$, $(a \cdot b) \cdot c=a \cdot(b \cdot c)$
composing two lists of moves puts us in a state that can itself be described by a list of moves
in both cases the combined ordered list of moves is the same
identity: there is an element in G call it 1 - such that for each $a$ in G, $1 \cdot a$ $=a \cdot 1=a$
the identity is the element corresponding to the solved state itself (empty list of moves)
inverse: for each $a$ in $G$, there exists $a^{-1}$ in $G$ such that $a \cdot a^{-1}=a^{-1} \cdot a=1$
closure: for all $a, b$ in $G, a \cdot b$ is in $G$
associativity: for all $a, b, c$ in $G$, $(a \cdot b) \cdot c=a \cdot(b \cdot c)$
composing two lists of moves puts us in a state that can itself be described by a list of moves
in both cases the combined ordered list of moves is the same
identity: there is an element in G call it 1 - such that for each $a$ in $G, 1 \cdot a$ $=a \cdot 1=a$
inverse: for each $a$ in $G$, there exists $a^{-1}$ in $G$ such that $a \cdot a^{-1}=a^{-1} \cdot a=1$
the identity is the element corresponding to the solved state itself (empty list of moves)
each individual move can be reversed and the whole list can be performed backwards


## But why bother with all this?

- Now we can use all the stuff that mathematicians have proved about groups! Tools for discovering and classifying internal structure, subgroups, symmetry, etc.
- group theory is pretty much the study of symmetry...
- "the power of group theory to abstractly formalize why everything sucks" - a mathematician friend of mine
- The authors of this paper took advantage of a much smaller subgroup to guide their search and avoid a lot of redundant computation.


## I wish we had time for more group stuff

- Maybe more in an optional puzzle / problem set?
- If this sounds intriguing, consider taking:
- Math 109 (as an elective for the CS major)
- Math 120 (if you plan to major in math or do more algebra stuff)


## ABSTRACT

ALGEBRA

