Introduction to Discrete Math

Felipe P. Vista IV

Course Outline

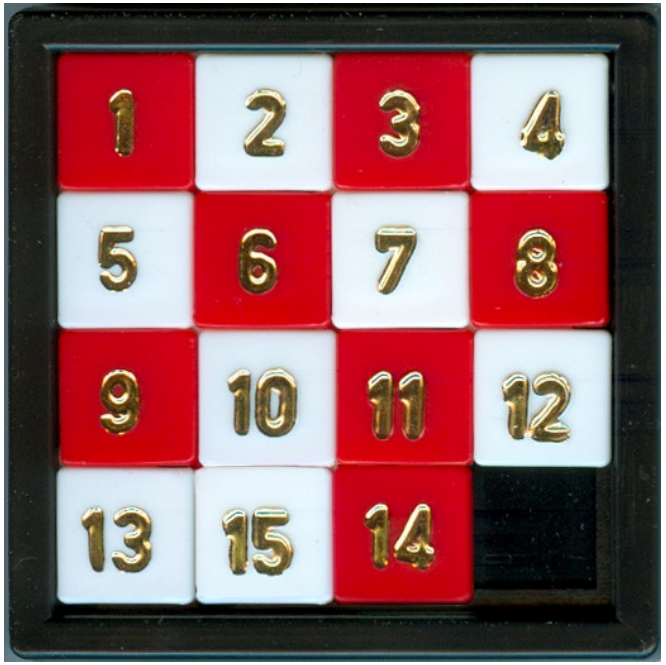
- Mathematical Thinking
  - Convincing Arguments, Find Example, Recursion, Logic, Invariants
- Probability & Combinatronics
  - Counting, Probability, Random Variables
- Graph Theory
  - Graphs (cycles, classes, parameters)
- Number Theory & Cryptography
  - Arithmetic in modular form
  - Intro to Cryptography

Mathematical Thinking – Invariants

THE 15-PUZZLE

- The game
- Permutations
- Proof: The Challenging Part
- Mission Impossible
- Classify a Permutation

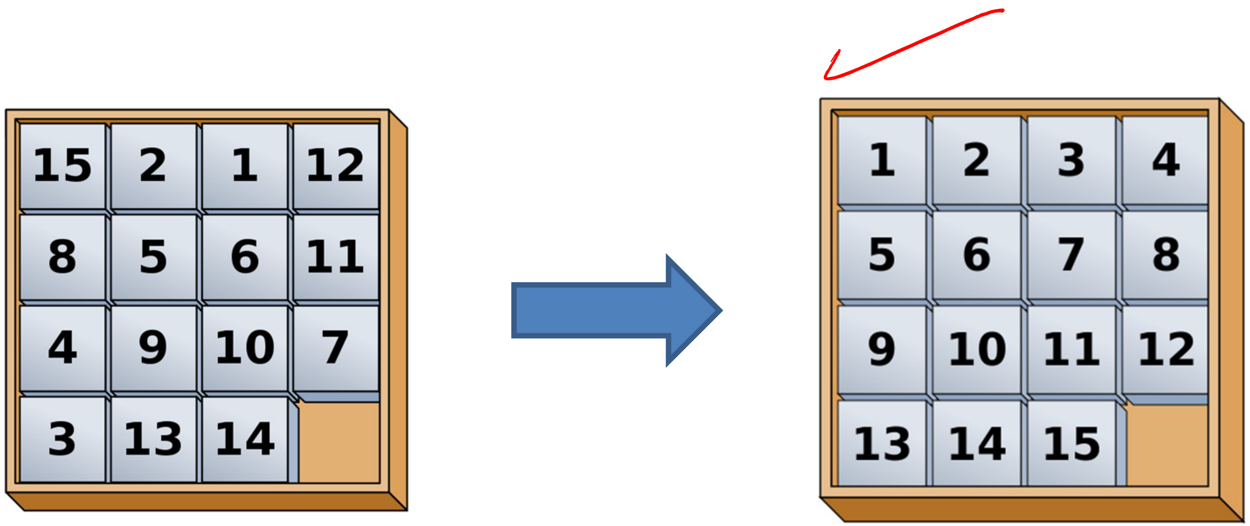
The 15-Puzzle



https://upload.wikimedia.org/wikipedia/commons/4/48/15-Puzzle.jpg

The Game

- move the pieces (into an empty neighbor square)
- goal → to obtain a particular configuration
- go back to starting configuration



https://upload.wikimedia.org/wikipedia/commons/thumb/f/ff/15-puzzle_magical.svg/800px-15-puzzle_magical.svg.png

https://i.stack.imgur.com/0B14h.png

The Game

- move the pieces (into an empty neighbor square)

The Game

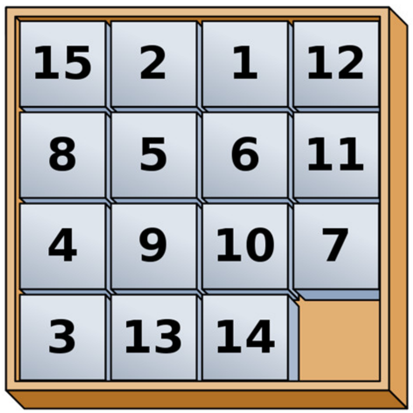
- move the pieces (into an empty neighbor square)
- goal → to obtain a particular configuration

The Game

- move the pieces (into an empty neighbor square)
- goal → to obtain a particular configuration
- go back to starting configuration

The Game

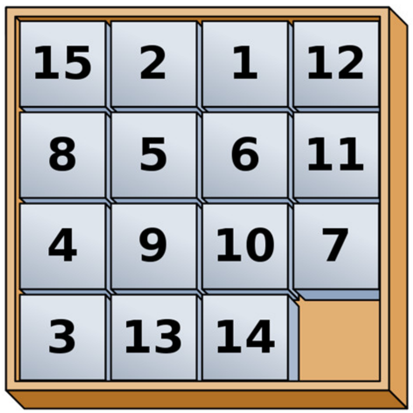
- move the pieces (into an empty neighbor square)
- goal → to obtain a particular configuration
- go back to starting configuration



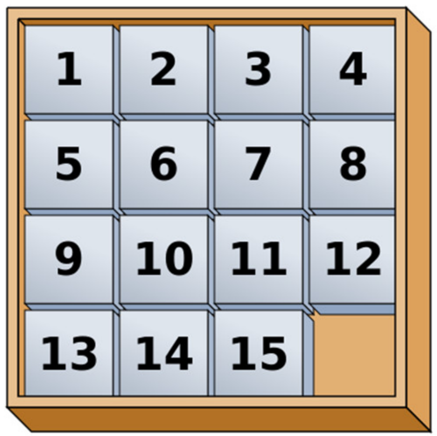
https://upload.wikimedia.org/wikipedia/commons/thumb/f/ff/15-puzzle_magical.svg/800px-15-puzzle_magical.svg.png

The Game

- move the pieces (into an empty neighbor square)
- goal → to obtain a particular configuration
- go back to starting configuration



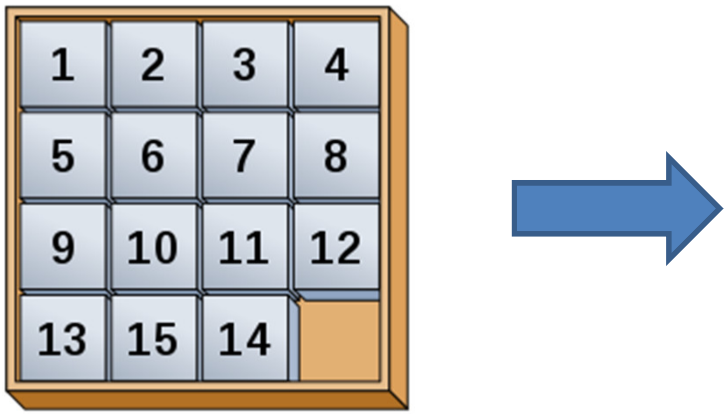
https://upload.wikimedia.org/wikipedia/commons/thumb/f/ff/15-puzzle_magical.svg/800px-15-puzzle_magical.svg.png



https://i.stack.imgur.com/0B14h.png

The Game

- move the pieces (into an empty neighbor square)
- goal → to obtain a particular configuration
- go back to starting configuration
- Are you up to it?



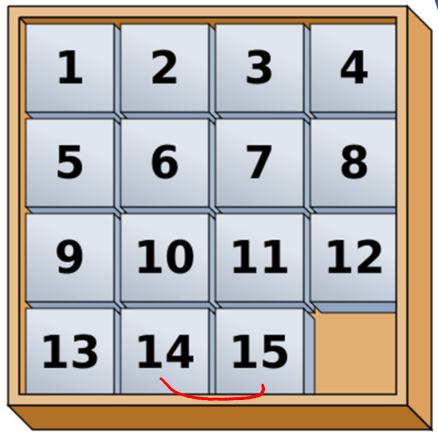
https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/15-puzzle-loyd.svg/600px-15-puzzle-loyd.svg.png

The Game

- move the pieces (into an empty neighbor square)
- goal → to obtain a particular configuration
- go back to starting configuration
- Are you up to it?

$100 Dare!

https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/15-puzzle-loyd.svg/600px-15-puzzle-loyd.svg.png



https://i.stack.imgur.com/0B14h.png

History

- invented in the 19th century

History

- invented in the 19th century
- complicated claims (Chapman, Sam Loyd)

History

- invented in the 19th century
- complicated claims (Chapman, Sam Loyd)
- very popular for some time, prizes were offered!

History

- invented in the 19th century
- complicated claims (Chapman, Sam Loyd)
- very popular for some time, prizes were offered!
- why take risk of giving prize (15-14 interchanged):

History

- invented in the 19^{th} century
- complicated claims (Chapman, Sam Loyd)
- very popular for some time, prizes were offered!
- why take risk of giving prize (15-14 interchanged):
  - impossibility proof exists!

History

- invented in the 19th century
- complicated claims (Chapman, Sam Loyd)
- very popular for some time, prizes were offered!
- why take risk of giving prize (15-14 interchanged):
  - impossibility proof exists!
- Challenge: reinvent this proof!

History

- invented in the 19th century
- complicated claims (Chapman, Sam Loyd)
- very popular for some time, prizes were offered!
- why take risk of giving prize (15-14 interchanged):
  - impossibility proof exists!
- Challenge: reinvent this proof!

https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/15-puzzle-loyd.svg/600px-15-puzzle-loyd.svg.png

https://i.stack.imgur.com/0B14h.png

- The game
- Permutations
- Proof: The Challenging Part
- Mission Impossible
- Classify a Permutation

Another point of view

- Empty cell active

Another point of view

- Empty cell active
  - move around, exchange places with neighbors

Another point of view

- Empty cell active
  - move around, exchange places with neighbors
- Generally:

Another point of view

- Empty cell active
  - move around, exchange places with neighbors
- Generally:
  - permutations of n objects obtained through sequence of pair exchanges (transpositions)

Another point of view

- Empty cell active
  - move around, exchange places with neighbors
- Generally:
  - permutations of n objects obtained through sequence of pair exchanges (transpositions)
  - STOP → SPOT:

Another point of view

- Empty cell active
  - move around, exchange places with neighbors
- Generally:
  - permutations of n objects obtained through sequence of pair exchanges (transpositions)
  - STOP → SPOT:
    - one transposition enough

Another point of view

- Empty cell active
  - move around, exchange places with neighbors
- Generally:
  - permutations of n objects obtained through sequence of pair exchanges (transpositions)
  - STOP → SPOT:
    - one transposition enough
  - STOP →POST:

STOP → SPOT

STOP → POST

steps?

Another point of view

- Empty cell active
  - move around, exchange places with neighbors
- Generally:
  - permutations of n objects obtained through sequence of pair exchanges (transpositions)
  - STOP → SPOT:
    - one transposition enough
  - STOP →POST:
    - how many transposition?

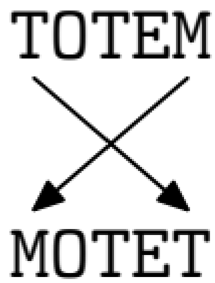
STOP → POST
SPTOS
POTS
POST

Even and Odd Permutations

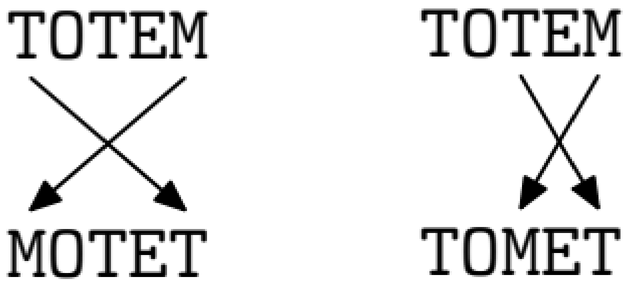
- STOP $\rightarrow$ SPOT: 1, 3, 5, 7, …
- STOP $\rightarrow$ POST: 3, 5, 7, …
- STOP $\rightarrow$ POTS: 2, 4, 6, …
- n + n transposition: twice nothing
- Conjecture: permutations are two types
  - Even
  - Odd

A Counterexample

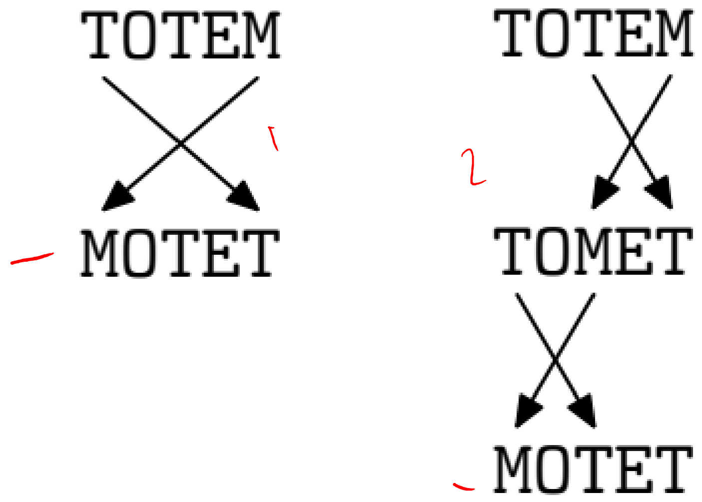
A Counterexample



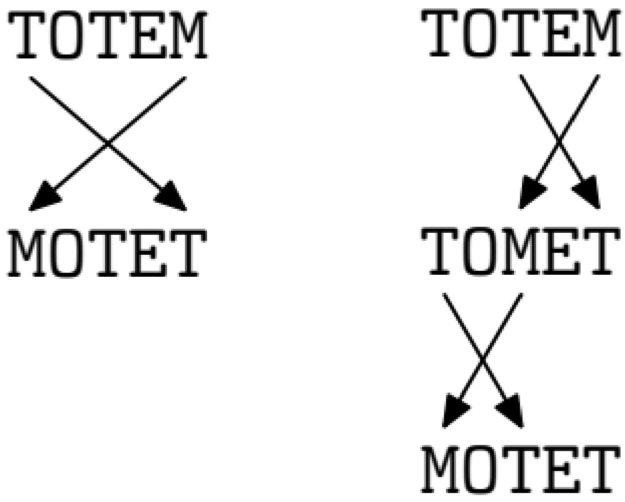
A Counterexample



A Counterexample

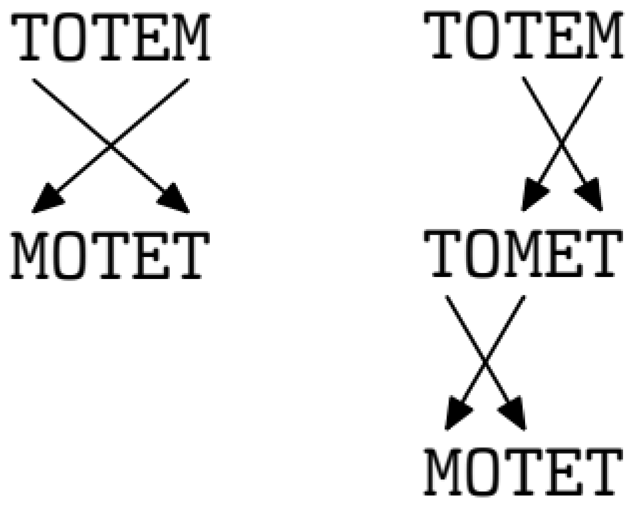


A Counterexample



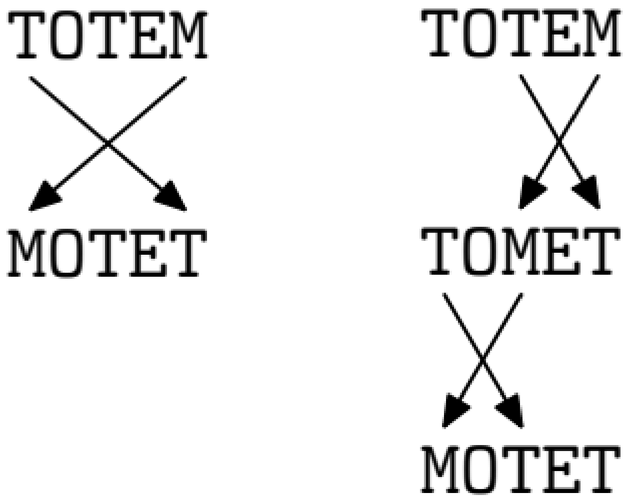
- even and odd at the same time?

A Counterexample



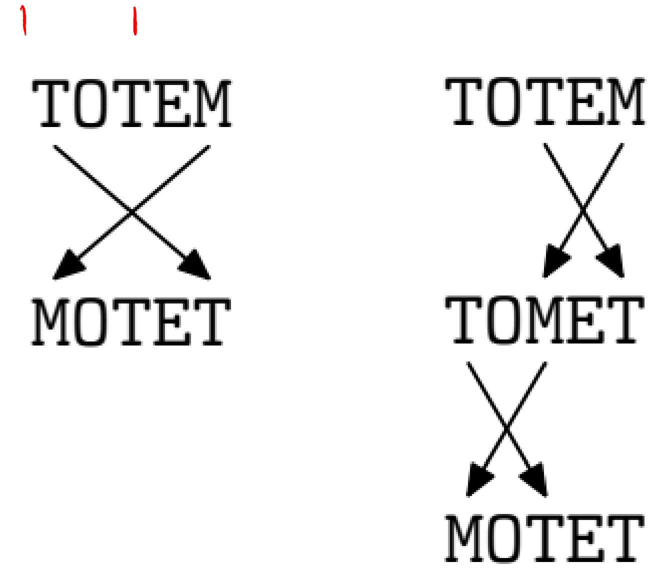
- even and odd at the same time?
- spoiler!

A Counterexample



- even and odd at the same time?
- spoiler!
  - two T's are mixed (we assumed all letters are different)

A Counterexample



- even and odd at the same time?
- spoiler!
  - two T's are mixed (we assumed all letters are different)

Theorem

Theorem

STOP → STPO
SOTP

- each permutation can be obtained through transpositions

Theorem

- each permutation can be obtained through transpositions
- some permutations can be derived only through an even number of transpositions, while others can be derived only through odd number of transpositions

Proof: The Easy Part

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

$$\mathrm{STOP} \rightarrow \mathrm{POST}$$

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

STOP → POST
STOP

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

STOP → POST

STOP

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

STOP → POST

STOP

PTOS

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

STOP → POST

STOP

PTOS

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

STOP → POST

STOP

PTOS

POTS

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

STOP → POST
STOP
PTOS
POTS

Proof: The Easy Part

- claim: each permutation can be obtained by transpositions
- proof: put letters to their right place through one transposition per letter

permutation

STOP → POST

STOP

PTOS

POTS

POST

Thank you.