CS 6041
Theory of Computation

Introduction

Kun Suo

Computer Science, Kennesaw State University

https://kevinsuo.github.io/

Outline

- Basic conceptions
  - Set and elements
  - Set operation
  - String and language
  - Boolean operation
- Types of proof
  - Construction
  - Contradiction
  - Induction

Set and element

- **Set**: a group of objects represented as a unit
  - E.g., natural number *N*, integers *Z*, empty set Ø
- **Element/member**: the object in a set
  - E.g., $1 \in N$
- **Subset**: if every member of A is also a member of B
  - E.g., $\{1,2,3\} \subseteq N$

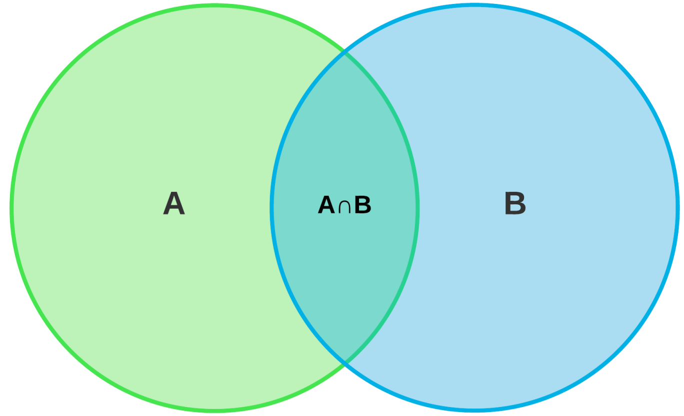
Set operations

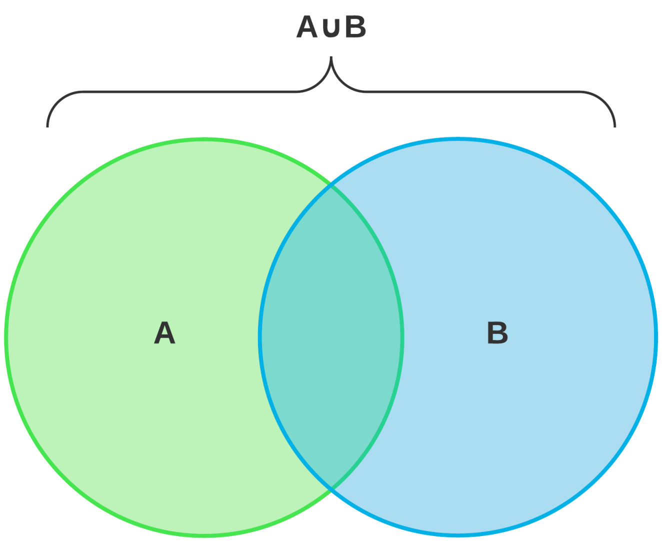
- **Union**: combine all elements in two sets into a single set
  - E.g., $A = \{1\},\ B = \{2\},\ A \cup B =\ ?$
- **Intersection**: the set of elements that are in both sets
  - E.g., $A = \{1,2,3\},\ B = \{2,3,4\},\ A \cap B =\ ?$
- **Complement**: the set of all elements that not are not in one set
  - E.g., $A = \{1,3,5, \dots\},\ \bar{A} = ?$ $\quad$ Suppose $U\ is\ N$

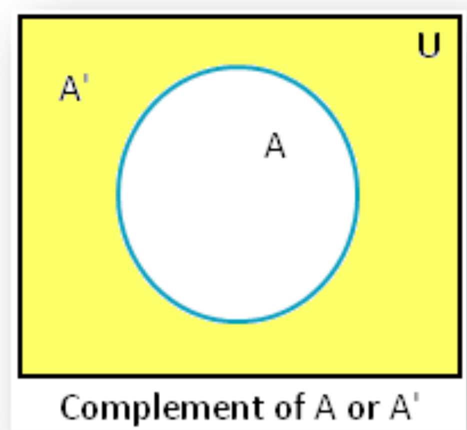
Set operations

- **Union**: combine all elements in two sets into a single set
  - E.g., $A = \{1\},\ B = \{2\},\ A \cup B = \{1,2\}.$
- **Intersection**: the set of elements that are in both sets
  - E.g., $A = \{1,2,3\},\ B = \{2,3,4\},\ A \cap B = \{2,3\}.$
- **Complement**: the set of all elements that not are not in one set
  - E.g., $A = \{1,3,5, \dots\},\ \bar{A} = \{0,2,4,6, \dots\}$

Venn diagram







Complement of A or A'

Sequence

- Sequence: a list of objects in some order
  - $\{7, 21,33\}$

- Tuple: a finite sequence
  - Is $\{7, 21,33\}$ a tuple?
    - Yes, it is a 3-tuple
  - Is $\{1,3,5, \ldots\}$ a tuple?
    - not tuple

Sequence

- Cross product: A x B, the set of all ordered pairs wherein the first element is a member of A and the second element is a member of B
  - $A = \{1,2\}$, $B = \{x,y,z\}$, $A \times B =$

    $\{ (1, x), (1, y), (1, z), (2, x), (2, y), (2, z) \}$

- $A^k = A \times A \times \ldots \times A$, (there are k As)

String

- Alphabet: any non-empty finite set
  - $\Sigma = \{0,1\}, \;\; \Sigma = \{a, b, c, d, \dots, z\}$

- String: a finite sequence of symbols
  - $x = 01001, w = university$

String

- Concatenation: append one string to another
  - If $x = 01001$, $w = university$
  - $xw = \quad 01001university$
  - $xx = x^2 = \quad 0100101001$

String

- Length, $x = 01001, w = university$
  - What is the length of x, w, xw?
    - |x|=5, |w|=10, |xw|=15

- Empty string: the string of length 0
  - $|\varepsilon| = 0, \quad x^0 = \varepsilon$

String

- Substring: a string consecutively within another string, w=$university$
  - $sity$ is a substring of w

- Subsequence: a sequence consecutively within another sequence
  - {u, v, s} is a subsequence of w

Language

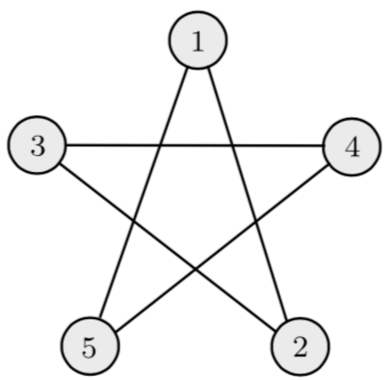
- Language: a set of strings
- Empty language: $\emptyset$
  - Empty string language: $\{\varepsilon\}$
  - Empty string: ε
- Concatenation on language
  - $AB = \{xy \mid x \in A \text{ and } y \in B\}$
  - $\{\varepsilon\}A = A\{\varepsilon\} = A$
  - $\emptyset A = A\emptyset = \emptyset$

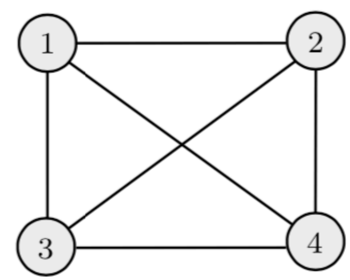
Lexicographic ordering

- Lexicographic ordering (Shorter strings precede longer strings) of all string over {0, 1} is
  - $\{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$

Graph

- An undirected graph, or simply a graph, is a set of points with lines connecting some of the points.
- The points are called nodes
- the lines are called edges

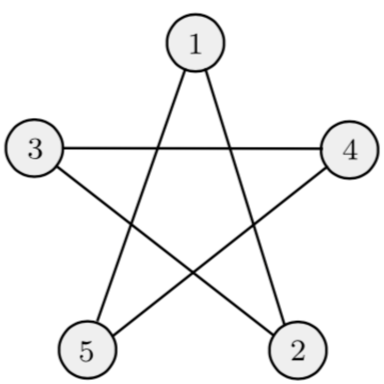




Graph

- The number of edges at a particular node is the ***degree*** of that node.

- We can describe a graph (V, E) with a diagram or more formally by specifying V and E.



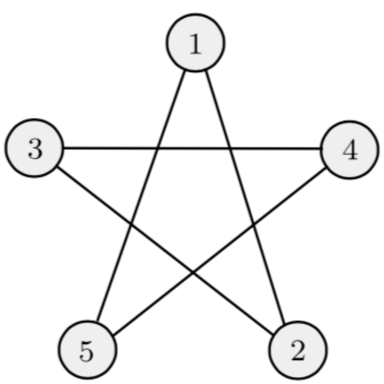
What is the degree of node 3?

Write the description of left figure?

Graph

- The number of edges at a particular node is the ***degree*** of that node.

- We can describe a graph (V, E) with a diagram or more formally by specifying V and E.

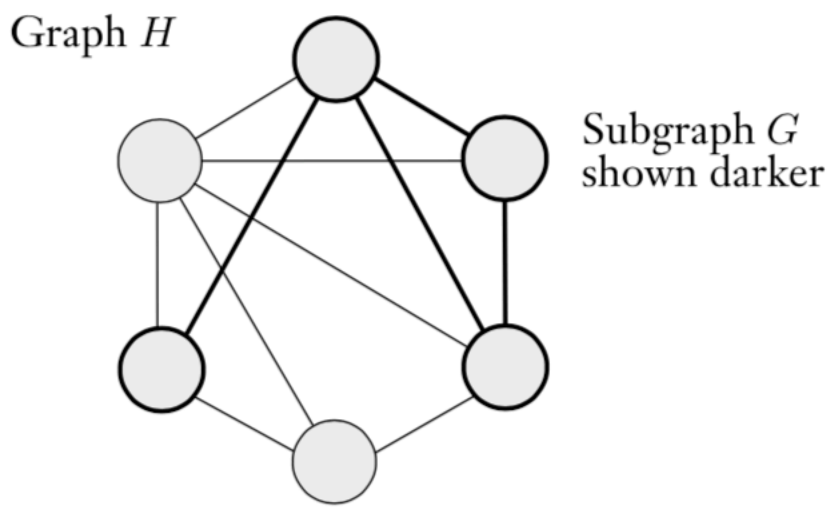


all the nodes have degree 2

({1, 2, 3, 4, 5}, {(1, 2), (2, 3), (3, 4), (4, 5), (5, 1)})

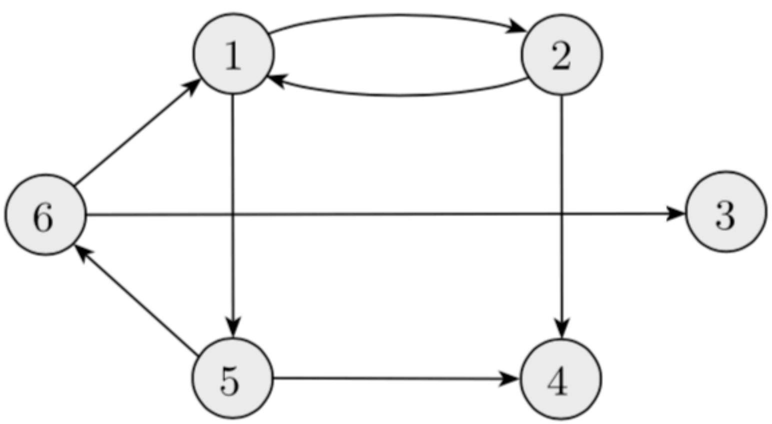
Graph

- Graph G is a ***subgraph*** of graph H if the nodes of G are a subset of the nodes of H, and the edges of G are the edges of H on the corresponding nodes.



Directed graph

- A directed graph has arrows instead of lines
- The number of arrows pointing from a particular node is the ***outdegree*** of that node
- The number of arrows pointing to a particular node is the ***indegree*** of that node

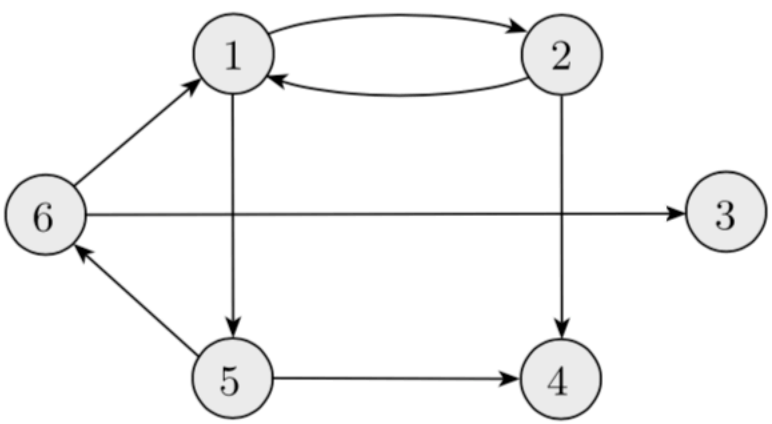


Indegree of {6} = ?
Outdegree of {6} = ?

Description?

Directed graph

- A directed graph has arrows instead of lines
- The number of arrows pointing from a particular node is the ***outdegree*** of that node
- The number of arrows pointing to a particular node is the ***indegree*** of that node



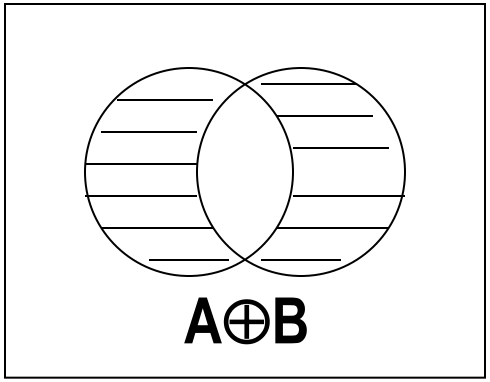
Indegree of {6} = 1
Outdegree of {6} = 2

({1,2,3,4,5,6}, {(1,2), (1,5), (2,1), (2,4), (5,4), (5,6), (6,1), (6,3)})

Boolean logic and operation

- OR
  - $0 \vee 0 = 0$
  - $1 \vee 0 = 1$
- AND
  - $0 \wedge 1 = 0$
- NOT
  - $\neg 0 = 1$
- XOR
  - $0 \oplus 0 = 0$
  - $0 \oplus 1 = 1$
  - $1 \oplus 1 = 0$

Result is true when X and Y are different



symmetric difference

Types of proof

- Proof by construction
  - Create a formula, graph, automata, Turing machine …
- Proof by contradiction
  - $\sqrt{2}$ is irrational
- Proof by induction
  - P(1) is true
  - Suppose P(n) is true, prove P(n+1) based on P(n)

Proof by construction definition

- Many theorems state that a particular type of object exists. One way to prove such a theorem is by demonstrating how to construct the object. This technique is a <u>proof by construction</u>.

Proof by construction example

- Prove: "There exist positive integers that can be expressed in two ways as the sum of cubic numbers.”

- Proof:

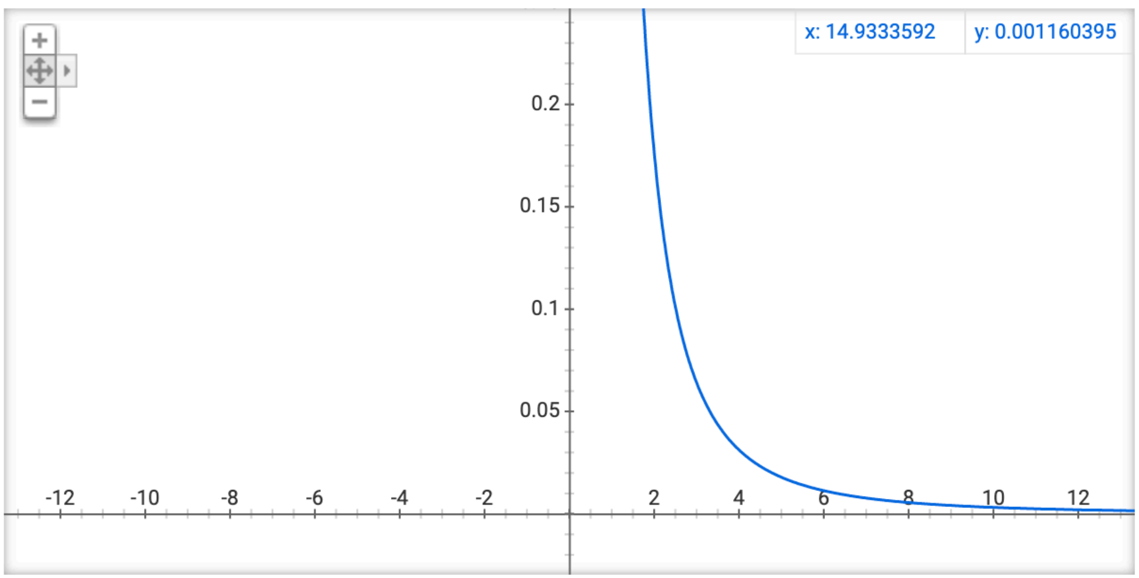
$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

Proof by construction example

- Compare which one is larger: $3^{-\frac{5}{2}}$ and $3.1^{-\frac{5}{2}}$
- Proof:

Create power function $y = x^{-\frac{5}{2}}$

Graph for x^-2.5



https://www.google.com/search?q=y%3Dx%5E(-2.5)&oq=y%3D&aqs=chrome.2.69i57j0j69i59j0l2j69i65.2872j0j7&sourceid=chrome&ie=UTF-8

$$3^{-\frac{5}{2}} > 3.1^{-\frac{5}{2}}$$

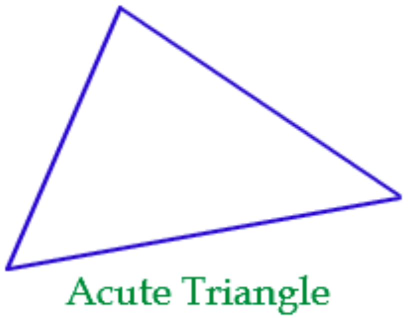
Proof by contradiction definition

- In one common form of argument for proving a theorem, we assume that the theorem is false and then show that this assumption leads to an obviously false consequence, called a contradiction. This technique is a <u>proof by contradiction</u>.

Proof by contradiction example

- Prove: if triangle ABC is an acute triangle (each angle is less than 90^o) and $\angle A > \angle B > \angle C$, then $\angle B > 45^o$

- Proof:



Suppose $\angle B \leq 45^o$

$\because \angle C < \angle B \leq 45^o$

$\therefore \angle B + \angle C < 2 \times \angle B \leq 90^o$

$\because \angle A + \angle B + \angle C = 180^o$, then

$\angle A = 180^o - \angle B - \angle C \geq 180^o - 90^o = 90^o$, which is contradicted with ABC is an acute triangle.

Proof by contradiction example

- Prove: square root $\sqrt{2}$ is irrational

- Proof:

Suppose $\sqrt{2}$ is rational , then $\sqrt{2}$ can be expressed as $\frac{m}{n}$, m and n are not even at the same time

Then n $\sqrt{2}$ = m

$2n^2 = m^2$ (square both sides)

Proof by contradiction example

- Prove: $\sqrt{2}$ is irrational

- Proof:

  $2n^2 = m^2$ (square both sides)

  m^2 is twice of n^2 and m must be even number

  Suppose $m=2k$

  Then $2n^2 = m^2 = 4k^2$

  $n^2 = 2k^2$, and n is also an even number, which is contradicted with "m, n are not even at the same time".

Proof by induction definition

- Proof by induction is an advanced method used to show that all elements of an infinite set have a specified property.

- Every proof by induction consists of two parts:
  1. basis step: proves that $P(1)$ is true.
  2. induction step: proves that for each $i \geq 1$, if $P(i)$ is true, then so is $P(i + 1)$.

Proof by induction example

- Prove: 3^n-1 is an even number

- Proof:

  1, let n=1,

  Then 3-1=2, is even

  2, suppose when n=k, 3^k-1 is even, then

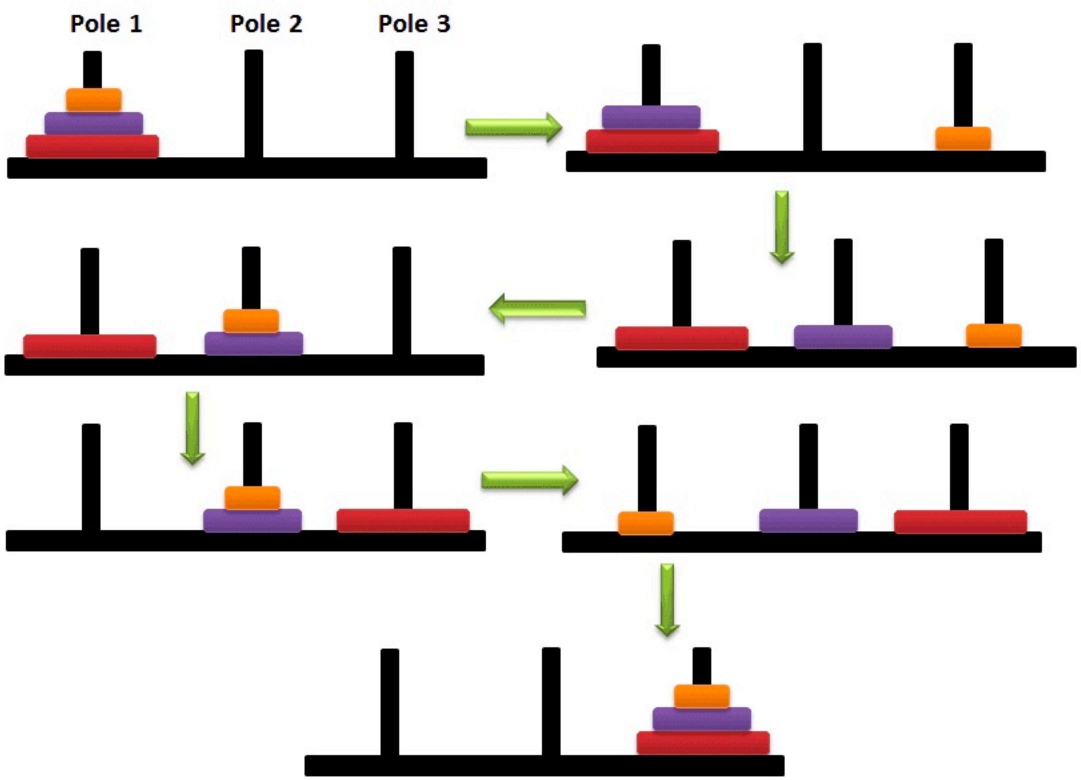
  $3^{k+1} - 1 = 3 x 3^k - 1$

  $= 2 x 3^k + 3^k - 1$

  Based on the assumption of n=k, 3^n-1 is also even for n=k+1

Proof by induction example

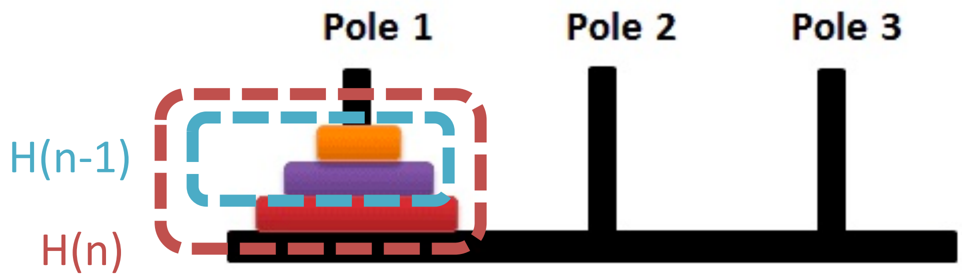
- Hanoi tower



Pole 1 has N disks. Each time we can only move one disk and the bigger disk cannot be put on top of smaller disks. How many moves do we need to move all disks from pole 1 to pole 3?

Proof by induction example

- Hanoi tower



$$H(n) = H(n-1) + 1 + H(n-1)$$

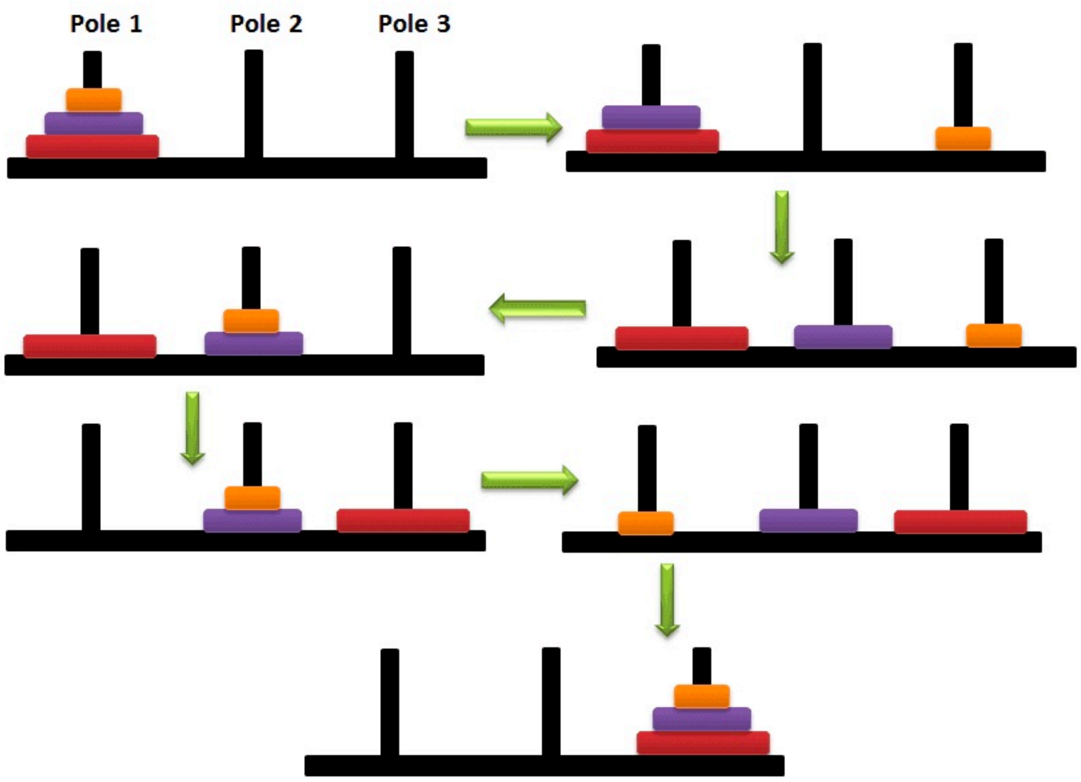
Move the top n-1 disks from pole 1 to pole 2

Move the bottom disk from pole 1 to pole 3

Move the top n-1 disks from pole 2 to pole 3

Proof by induction example

- Hanoi tower



$H(n) = 2^n - 1$

Conclusion

- Basic conceptions
  - Set and elements
  - Set operation
  - String and language
  - Boolean operation
- Types of proof
  - Construction
  - Contradiction
  - Induction