CSc 28
Discrete Structures

Chapter 1
Mathematical Induction

Herbert G. Mayer, CSU CSc

Status 1/10/2021

Syllabus

- Power Set
- Mathematical Induction
- A Distraction
- Strong Induction
- Recursion
- Towers of Hanoi
- References

Introduction

First we describe key mathematical terms essential to *Computer Science* studies, and to *Induction*

Then we discuss a delightful, small recursive program; but shall cover recursion and its SW implementation in detail later

Here we define & discuss:

- Set, Subset
- Power Set
- Universal Quantifier
- Logical, Mathematical Induction
- Infinite Series

Induction

- Here we discuss Mathematical Induction
- Induction is a technique used to prove statements, a formula, or a theorem; typically to be true for every natural number
- The technique involves two distinct steps to complete such a proof; these are
- Step 1: The Base Step proves that a statement is true for a specific, select, initial value
- Step 2: The Induction Step proves that if the statement is true for the n^{th} case, then it is also true for the n^{+1} case

Set

- In Mathematics, set is a clearly defined collection of distinct elements
- Elements of a set are AKA members
- Elements can be anything uniquely identifiable: e.g. people, letters of the alphabet, numbers, points in n-dimensional space, etc. even sets
- It is common for sets to have a name
- Two sets are equal if they contain exactly the same elements
- A set that has no elements is called an empty set
- More detail on sets in future chapter “Set Theory”

Power Set

- Definition: The Power Set P(S) of a set S is the set of all subsets of S including the empty set
- Example for set S = { a, b, c }:
  - The empty set { } is a subset of S
  - The following are some subsets of S: {a}, {b} and {c}
  - As are these: { a, b }, { a, c } and { b, c }
  - And also { c, b }, but is not distinct from set { b, c }
  - And { a, b, c } is a subset of S, but not a proper subset
  - Given n elements in set S, the number of elements in the Power Set P(S) is 2^n
- Jointly all these sets constitute the Power Set P(S):

P(S) = { {}, {a}, {b}, {c}, {a,b}, {a,c}, {b,c}, {a,b,c} }

Power Set

Power Set

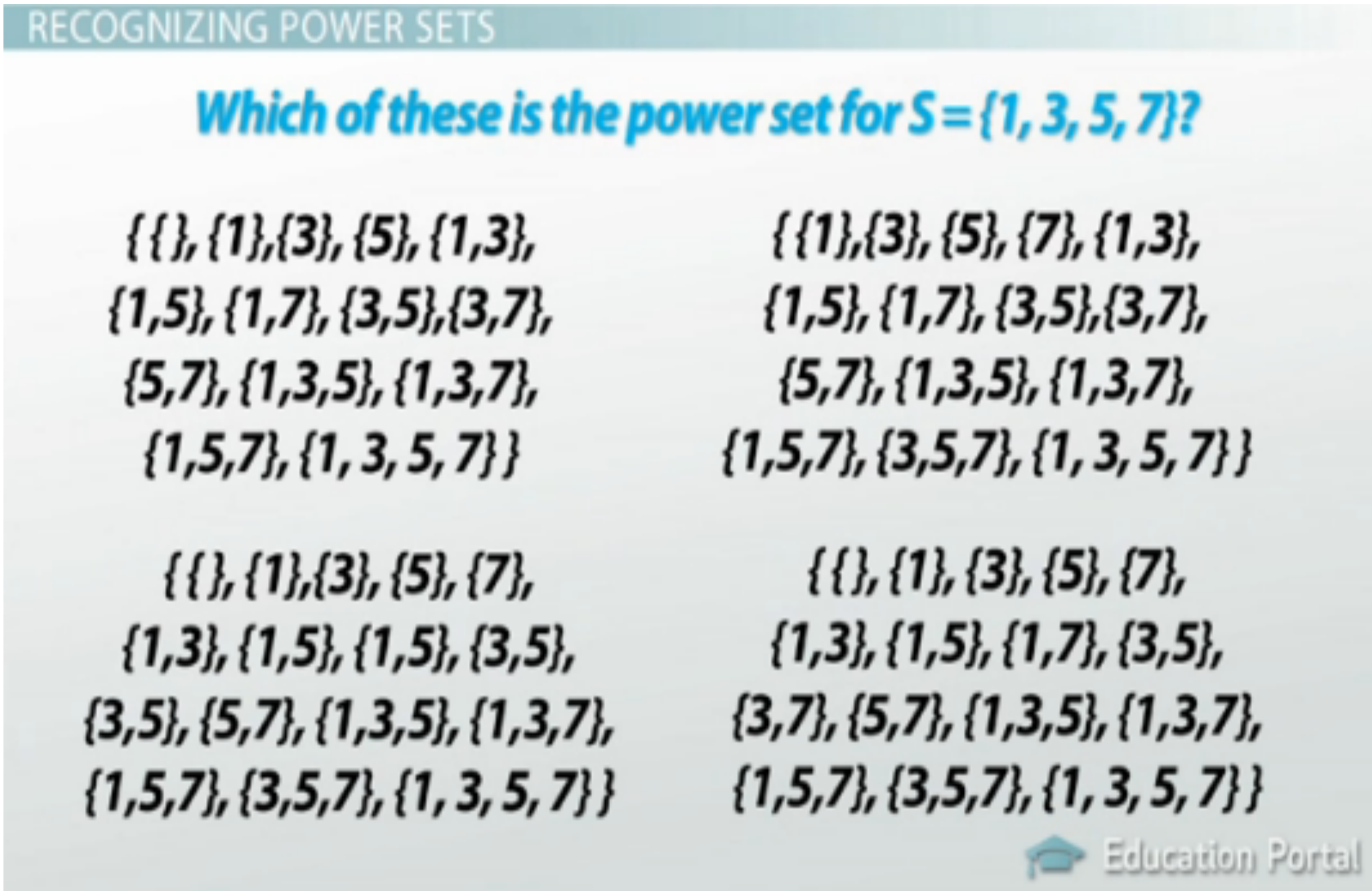
Power Set PS of a set S is the set of all possible distinct subsets of set S

Quick Exercise with specific set S below: How many elements are in the power set P(S) with set S being:

$$S = \{ 1, 3, 5, 7 \}$$

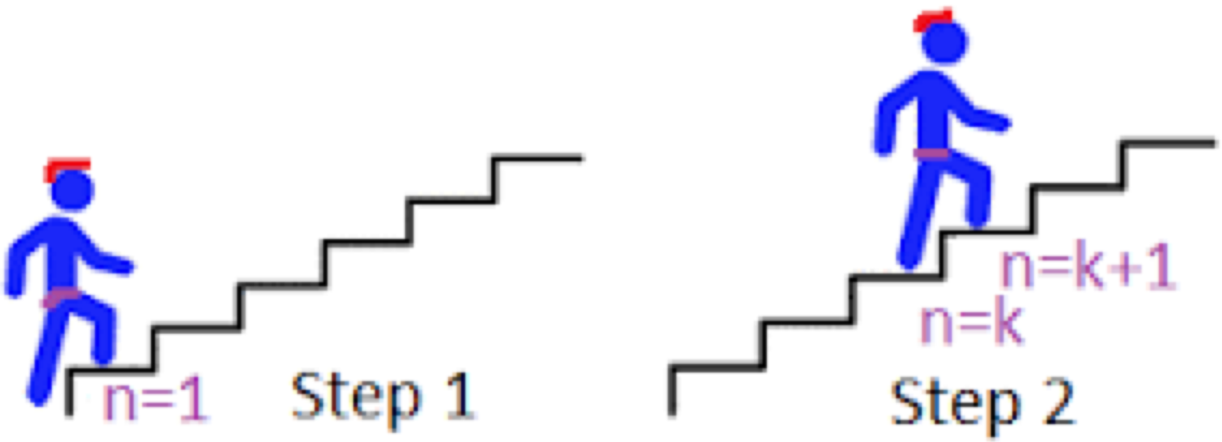
Power Set

Quick Exercise: Solve, first by counting: $2^4 = 16$ elements

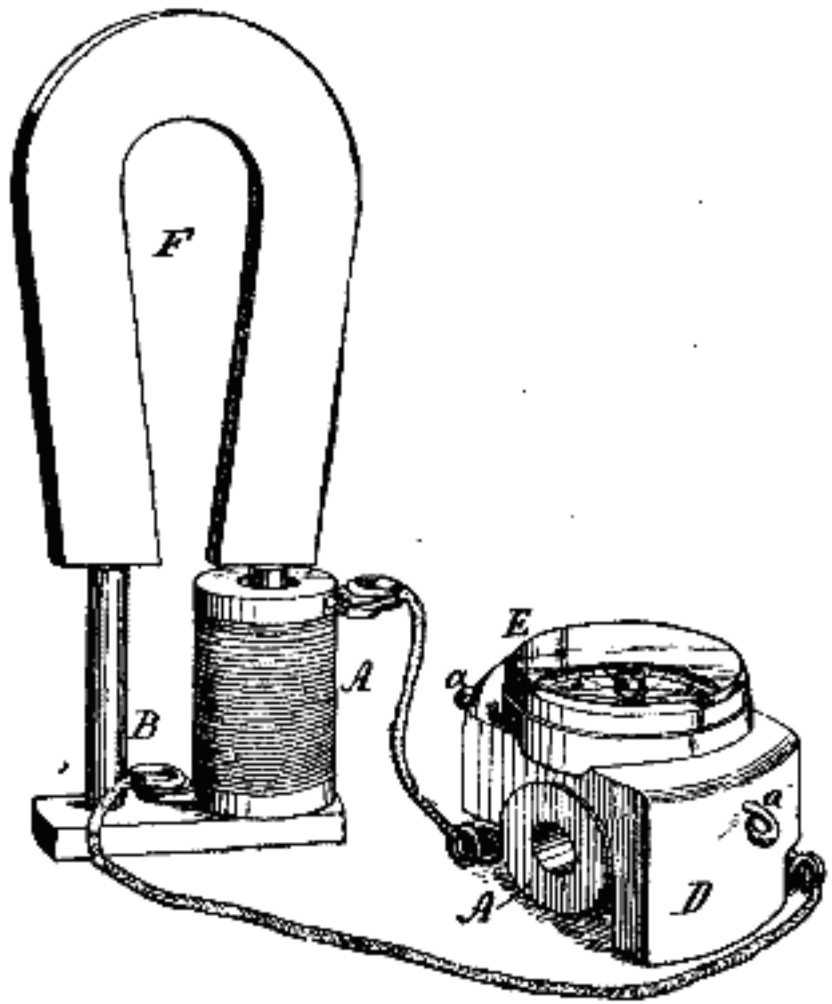


Induction

Logical Induction



Electrical Induction



Mathematical Induction

- The so called Universal Quantifier makes a general statement of truth; i.e. it is some statement that holds for all elements in some defined set
- Example 1: For every positive integer n we claim:

$$n! \leq n^n$$

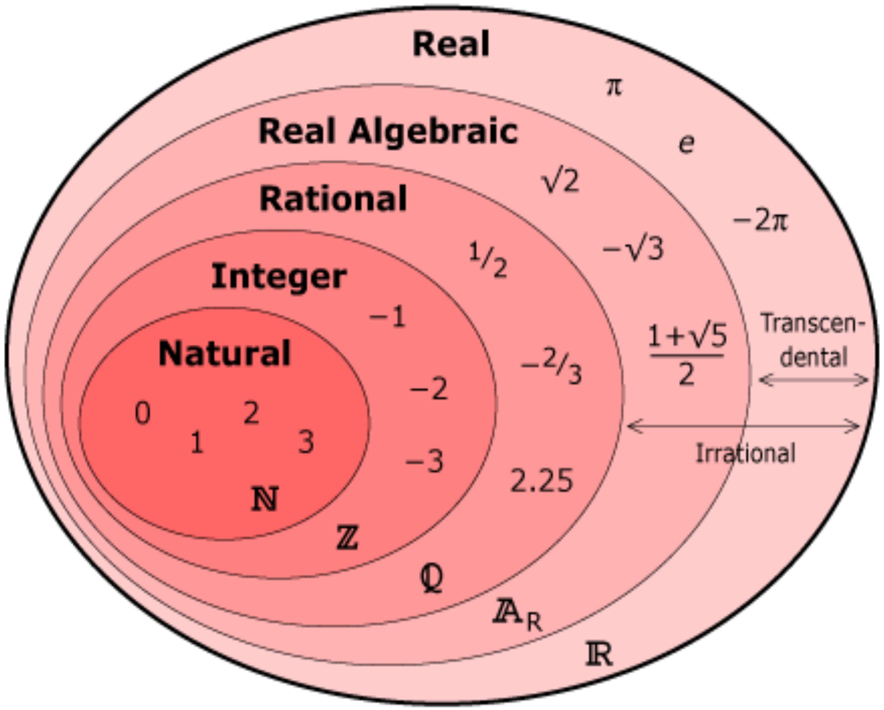
- But is this true? That is yet to be proven!
- Example 2: For every set S with n elements the cardinality of its power set P is:

$$\text{Cardinality}(\ P(S)\ ) = |P(S)| = 2^n$$

- Mathematical Induction (MI) is a key technique for proving universal statements about certain properties

Mathematical Induction

- **Mathematical Induction is a useful tool to prove some predicate to be true for a certain domain, typically for all natural numbers**
- **It cannot be used to discover new theorems; only to prove (or disprove) them**



Mathematical Induction

- Mathematical Induction takes 2 discrete steps
  - sometimes also described as 3 steps or even 4
- Step 1 is known as Base Case; step 2 the Induction Hypothesis, constituting the Induction Step
- The hypothesis clearly articulates the claim
- The steps are followed by a statement of conclusion, articulating what has just been proven
- The Base Case states that a property P clearly holds for some element, often indexed 0, AKA P(0)
- Could be another index, e.g. base case for index -1, or 0, or 1, etc. i.e. stating property P(-1), P(1) or P(2)

Mathematical Induction

- The **Induction Step** must show: since the property P(n) holds for some natural number *n*, then it also holds for *n+1*, AKA $\forall n \, (P(n) \rightarrow P(n + 1))$
- That has to be proven!
- This **n** is greater than the initial index identifying the **base case**; base case often being 0 or 1
- These steps establish the property P(n) for every natural number *n* = 0, 1, 2, 3, . . .
- Again, the base case **need not start with index 0**; for some formulae it begins with 1; can really be any natural number

Mathematical Induction

You likely have heard of *Domino Effect*

- **Step 1. The first domino falls**
- **Step 2. When any domino falls, the next domino falls**
- **Step 3. So . . . all dominos after the first will fall!**

Mathematical Induction Example 1

Example 1: Prove by induction that $S(n)$ the sum of the first $n \geq 1$ integers $1+2+3+4 \ldots +n$ is: $S(n) = n(n+1)/2$

- **Base Case** for 1: S(1) for n = 1:

  $$n(n+1)/2 = 1(1+1)/2 = 1 \text{ obviously true}$$

- The **Induction Hypothesis** argues: if it can be shown for $n > 1$ that $S(n)$ is true, then the **Induction Step** proves this same for $S(n+1)$ as well
- Assume there exists an n, $n > 1$ such that

  $$1 + 2 + \ldots + n = n(n+1)/2$$

- Referred to as the **inductive assumption**
- We must now prove correctness of the formula

  $$1 + 2 + \ldots + n + (n+1) = (n+1)(n+2)/2$$

Mathematical Induction Example 1

$1 + 2 + \ldots + n \qquad = n (n+1) / 2$

$1 + 2 + \ldots + n + (n+1) \qquad = n (n+1) / 2 + (n+1)$

$1 + 2 + \ldots + n + (n+1) \qquad = (n (n+1) + 2 (n+1)) / 2$

$1 + 2 + \ldots + n + (n+1) \qquad = (n+1)(n + 2) / 2$

$1 + 2 + \ldots + n + (n+1) \qquad = (n+1)((n+1) + 1) / 2$

q.e.d.

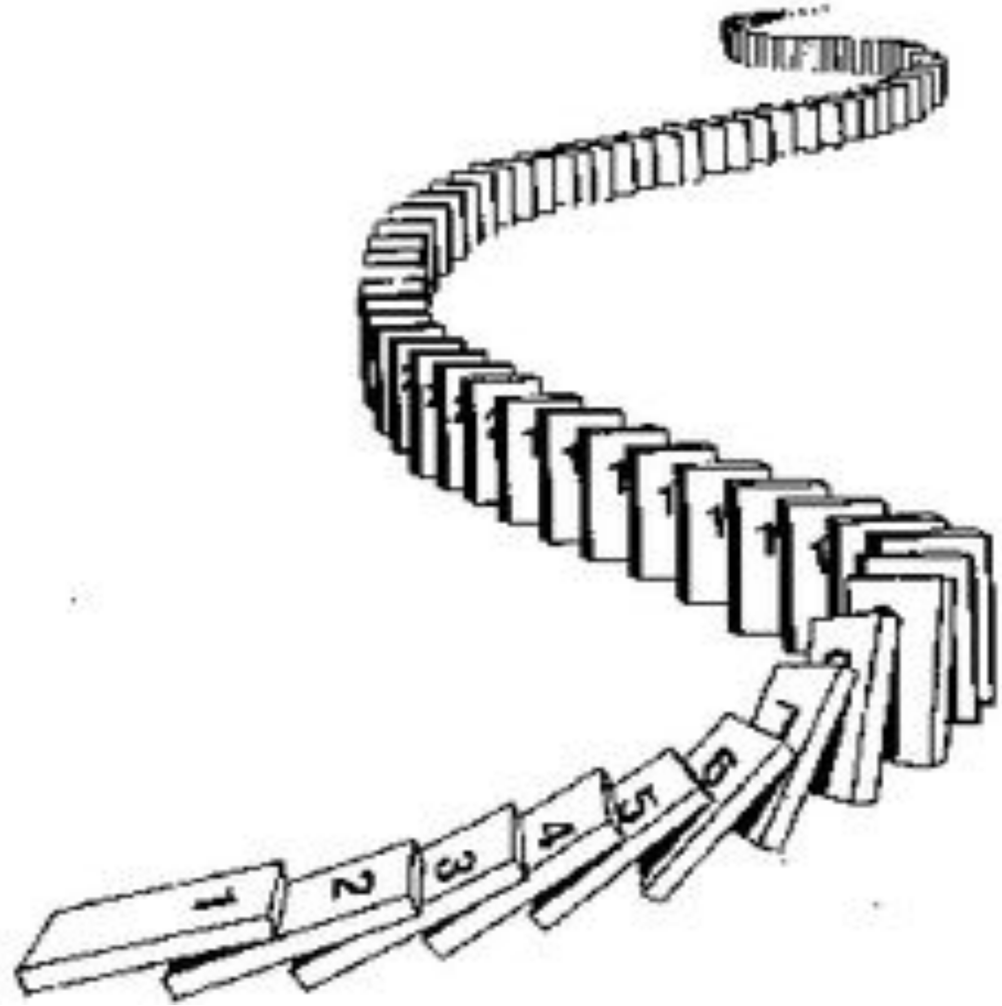
Easier to see, if we rename n+1 to k, i.e. $n+1 \equiv k$:

$1 + 2 + \ldots + n + (n+1) \qquad = (n+1)((n+1) + 1) / 2$

$1 + 2 + \ldots + n + k \qquad = k (k+1) / 2$

Choice of name n for the index is arbitrary

Dominos & Induction



Mathematical Induction Example 2

Example 2: Prove by induction that S(n) the sum of the first $n \geq 1$ odd integers is n^2

- I.e. we are adding up the first n odd integers, the sum named S(n), starting at 1
- They are valued: 1, 3, 5, 7 . . . (2n - 1)
- **Base Case S(1)** for n = 1: the sum of the first 1 odd integer is 1; claim is obvious, since $1 = 1^2$
- **Induction Step**: Assume that the sum S(n) of the first $n \geq 1$ odd integers is $= n^2$

Mathematical Induction Example 2

Example 2 Cont'd: Prove that S(n) the first $n \geq 1$ odd integers summed up is n^2

- Show that $\forall(n)\ (\ S(n) \rightarrow S(\ n+1\ )\ )$ By assumption for up to n: $1 + 3 + . . . + (2n - 1) = n^2$
- Then for case n+1:

$$1 + 3 + . . . + (2n-1) + (2n+1) = (n+1)^2$$

$$1 + 3 + . . . + (2n-1) + (2n+1) = n^2 + (2n + 1)$$

$$(n+1)^2 = n^2 + (2n + 1)$$

- Which happens to derive the well known binomial formula $(a+b)^2 = a^2 + 2ab + b^2$

q.e.d. ☺

Mathematical Induction Example 3

Example 3: Prove by induction that S(n) **sum of $n \geq 0$ powers of 2** is $2^{n+1} - 1$ for all non-negative integers n

- **Base Case S(0):** n = 0: $S(0) = 2^0 = 2^{n+1} - 1 = 2^{0+1} - 1 = 1$
- Base Case is obviously true!
- **Induction Step**: S(n) the sum of first n>0 powers of 2:
- $S(n) = 1 + 2 + 4 + \ldots 2^n = 2^{n+1} - 1$
- $S(n+1) = 1 + 2 + 4 + \ldots 2^n + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1}$
- $S(n+1) = 1 + 2 + 4 + \ldots 2^n + 2^{n+1} = 2 * 2^{n+1} - 1$
- $S(n+1) = 1 + 2 + 4 + \ldots 2^n + 2^{n+1} = 2^{n+2} - 1$

q.e.d.

Mathematical Induction Example 4

Example 4: Prove by induction that $11^n - 6$ is evenly divisible by 5 for every natural number $n > 0$

Expressed equivalently: $11^n - 6 = 5\,m$ for some integer m

Or: $11^n = 5\,m + 6$

- **Base Case** S(1) for n = 1: $11^1 - 6 = 5$
- Base case easily proven, as 5 is evenly divisible by 5
- **Induction Step** for $S(n) \rightarrow S(n+1)$:

  $11^n - 6 = 5\,m$ for some integer m

  $11^n = 5\,m + 6$ we use this version below

Mathematical Induction Example 4

$11^{n+1} - 6 = 11 * 11^n - 6$ --using * for clarity here

$11^{n+1} - 6 = 11 * (5 m + 6) - 6$

$11^{n+1} - 6 = 11 * 5 m + 66 - 6$

$11^{n+1} - 6 = 11 * 5 m + 60$

$11^{n+1} - 6 = 5 * 11 m + 60$

$11^{n+1} - 6 = 5 * (11 m) + 60$

$11^{n+1} - 6 = 5 * (11 m + 12)$

Since m is integer, $11 m + 12$ is integer, so we see that $11^{n+1} - 6$ is a multiple of 5, namely $11 m + 12$ times 5

q.e.d.

A Distraction

Is Correct Spelling Important?

I cdnuolt blveieetaht I cluod aulaclty uesdnatnrd waht I was rdanieg. The phaonmneal pweor of thehmuan mind. Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht thefrist and lsat ltteer be in the rghit pclae. The rset can be a taotl mses andyou can sitll raed it wouthit a porbelm.

Is Correct Spelling Important?

Tihs is bcuseeae the huamn mnid deosnot raed ervey lteter by istlef, but the wrod as a wlohe. Amzanig huh? yaeh and I awlyas thought slpeling was ipmorantt.

Is Correct Spelling Important?

- Not related to Induction ☹
- Used here to keep students awake ☺
- Text analysis, parsing sentences, language level analysis, grammars, linguistics are all highly important for CS
- See later in this class and in other, more advanced CS classes, specifically about grammars

Induction Continued

Mathematical Induction Example 5

Example 5: Prove the sum S(n) of the first n squares, varying i = 1..n is: $S(n) = n (n+1)(2n+1) / 6$

- **Base Case** S(1) for n = 1:

$$n (n+1)(2n+1) / 6 = 1 (1+1)(2+1) / 6 = 1$$

- **Induction Hypothesis** argues, if case holds for $n > 1$ and S(n) is true, then **Induction Step** proves this same claim for S(n+1) to be true as well
- **Induction Step:**

$$S(n) + (n+1)^2 = (n+1)((n+1) +1)(2 (n+1) + 1) / 6$$

$$n (n+1)(2n+1) / 6 + (n+1)^2 = (n+1)(n+2)(2n+3) / 6$$

Mathematical Induction Example 5

Example 5 Cont'd: Prove the first n squares, varying $i = 1..n$, to be $S(n) = n(n+1)(2n+1)/6$

$$n(n+1)(2n+1)/6 + (n+1)^2 = (n+1)(n+2)(2n+3)/6$$

$$n(n+1)(2n+1) + 6(n+1)^2 = (n+1)(n+2)(2n+3)$$

$$n(2n+1) + 6(n+1) = (n+2)(2n+3)$$

$$2n^2 + n + 6n + 6 = 2n^2 + 3n + 4n + 6$$

$$0 = 0$$

Obviously equal, thus the hypothesis is true

q.e.d.

Mathematical Induction Example 6

Example 6: Here we show a piece of mathematical trickery of exceptional beauty ☺. We prove by Induction that $7^n - 2^n$ is evenly divisible by 5 for any integer $n \geq 1$

- **Base Case for n = 1:**

  $7^n - 2^n = 7 - 2 = 5$ 5 is indeed an integral multiple of 5

- **The Induction Hypothesis assumes this also to be true for some $n > 1$**

- **Then we analyze whether it is also true for n+1, i.e. that $7^{n+1} - 2^{n+1}$ will be divisible by 5**

- **Instead of saying "is divisible by 5", we can also write: $7^n - 2^n = 5 * a$ for some quotient a, i.e. some natural number a**

Mathematical Induction Example 6

Example 6 Cont'd: Prove that $7^n - 2^n$ is evenly divisible by 5 for any $n \geq 1$; or equivalently: $7^n - 2^n = 5 * a$

- **Induction Step for n + 1**

$$7^{n+1} - 2^{n+1} = 7 * 7^n - 2 * 2^n$$

$$7^{n+1} - 2^{n+1} = 5 * 7^n + 2 * 7^n - 2 * 2^n$$

$$7^{n+1} - 2^{n+1} = 5 * 7^n + 2 * (7^n - 2^n)$$

$$7^{n+1} - 2^{n+1} = 5 * 7^n + 2 * 5 * a$$ -- see previous page

$$7^{n+1} - 2^{n+1} = 5 * (7^n + 2 * a)$$

And we know that $(7^n + 2 * a)$ is an integer expression, since all parts are integers!

q.e.d.

Mathematical Induction Exercise

Example 7: Prove that $n^n > n!$ for all $n > 1$

- **Base Case** for $n = 2$:

  $n^n = 2^2 = 4$; and $n! = 1 * 2 = 2$; base case is established

- The **Induction Hypothesis** argues, $n^n > n!$ for $n > 2$
- **Induction Step for n+1:**

Students do this on their own first

Mathematical Induction Exercise

Example 7: Prove that $n^n > n!$ for all $n > 1$

- **Base Case** for $n = 2$:

  $n^n = 2^2 = 4$; and $n! = 1 * 2 = 2$; base case is established

- The **Induction Hypothesis** argues, $n^n > n!$ for $n > 2$
- **Induction Step for n+1:**

$$(n+1)! = (n+1)n! < (n+1)n^n < (n+1)(n+1)^n$$

$$(n+1)(n+1)^n = (n+1)^{n+1}$$

$$(n+1)! < (n+1)^{n+1}$$

q.e.d.

Strong Induction

- We covered Induction, AKA Weak Induction; time to review a variant named Strong Induction
- Strong induction is quite similar to induction. Main difference: nature of the inductive hypothesis
- In weak Induction, we use knowledge of $P(n)$ being true to prove $P(n+1)$
- In strong induction, we verify P(1), P(2), P(3), . . . up to P(n) to prove P(n+1)
- Like with Induction, in Strong Induction initial index need not be 1
- Why go through such effort? Isn't it more economical to only have to prove one P(n)?

Strong Induction Example

Example 1: Prove that every integer $n > 1$ can be written as a product of prime numbers (primes starting at 2)

- **Base Case:** S(2) for n = 2: obvious!
- **Induction Hypothesis:** We assume that S(n) is true for n = 3, 4, 5, . . . N
- **Induction Step**:
- If next integer (n+1) is prime, the claim is confirmed
- Else (n+1) has a smallest prime factor p
  - (n+1) = p * N for some N < n and N ≤ p
  - But either N is prime or can be written as product of primes
  - Hence (n+1) can be written as a product of p * prime product

q.e.d.

Strong Induction

- Note the assumption alone S(n) was not sufficient in the proof
- We assumed S(2), etc. up to S(n) to prove S(n+1)
- It is not always necessary in Strong Induction to prove all cases 1 .. N
- But more than just one single case

Strong Induction Example

Example 2: A chocolate bar from **Lindt, Switzerland**, consists of a rectangular grid of m * n rows and columns of squares. Split the whole bar into all individual squares only by breaking along lines. Then $B(m, n) = m * n - 1$ individual breaks are required!

- **Base Case:** For a bar consisting of 1 square B(1,1) is obviously 0: $m * n - 1 = 1*1 - 1 = 0$
- **Induction Step**: Let $B(m, n)$ denote the number of breaks needed to split an $m * n$ bar
- If we break along a middle row, we get an $m_1 * n$ and an $m_2 * n$ bar, with $m_1 + m_2 = m$

Strong Induction Example

- If we break along a middle row, we get an $m_1 * n$ and an $m_2 * n$ bar, with $m_1 + m_2 = m$
- By induction hypothesis the number of further breaks needed is $m_1 * n - 1$ and $m_2 * n - 1$
- Hence the total number breaks needed B(m, n) is

$$B(m, n) = 1 + m_1 * n - 1 + m_2 * n - 1$$

$$B(m, n) = (m_1 + m_2) * n - 1$$

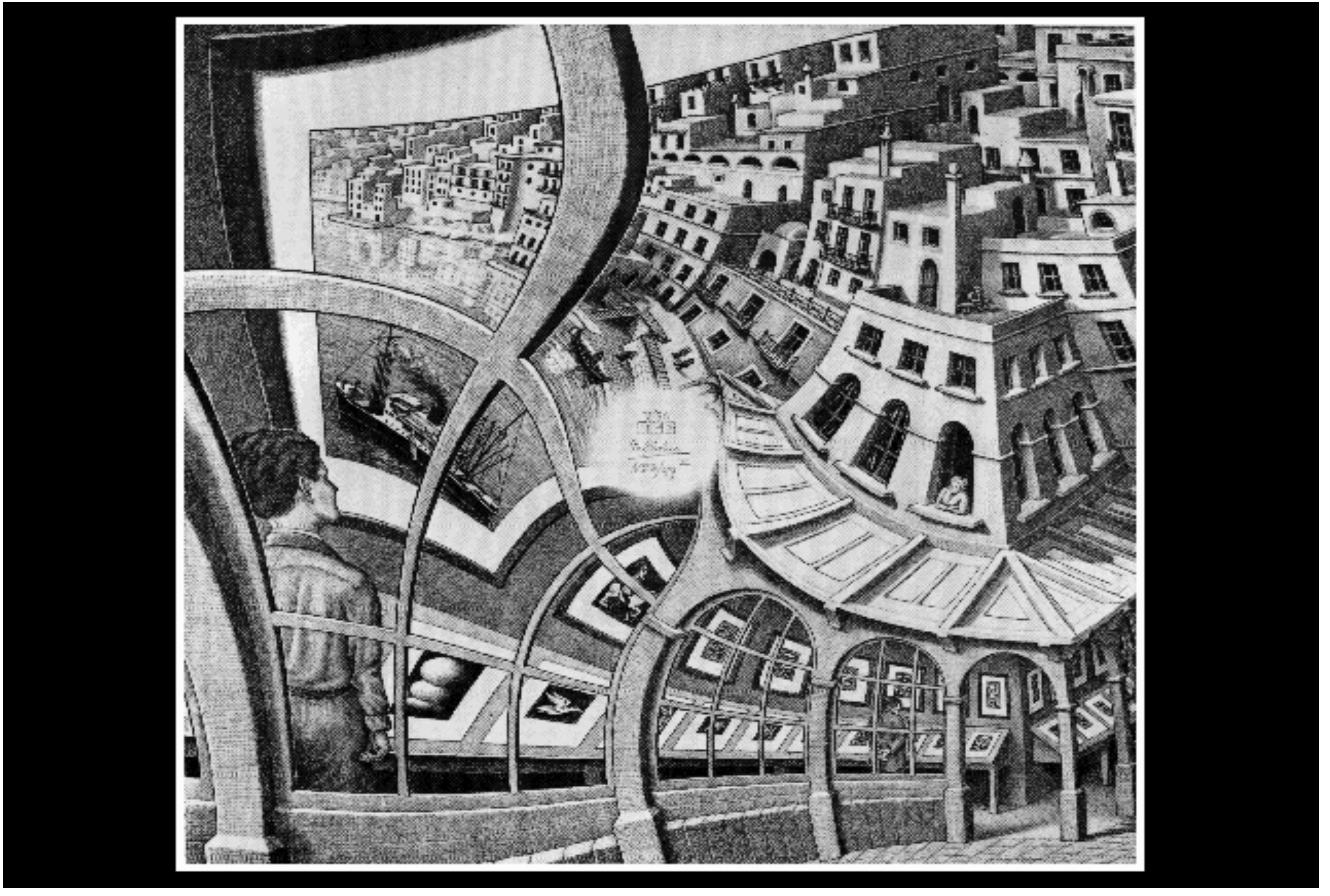
$$B(m, n) = m * n - 1$$

q.e.d.

- **Strong Induction** not further elaborated here

Recursion

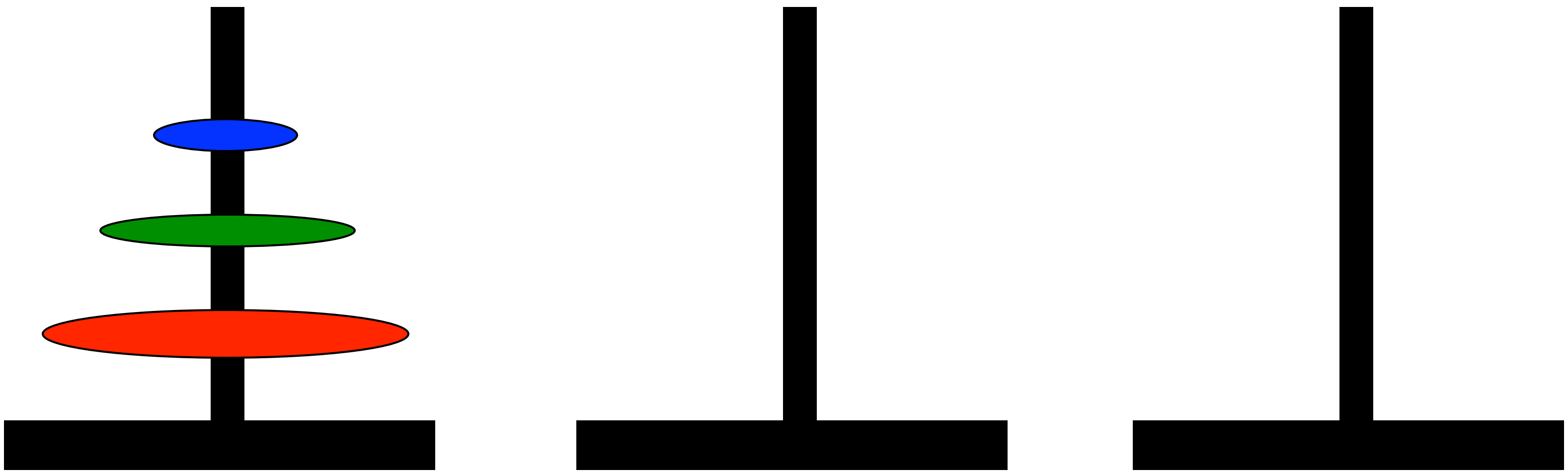
Recursion Introduction



Recursion

- **Definition: An algorithm is recursive, if it is partly defined in simpler versions of itself**
- **Note the “partly”: i.e. there are other parts to it, on top of the partly expressed recursive part**
- **Note the “simpler version”; this specifies some necessary condition for an algorithm to terminate eventually; i.e. to avoid infinite regress**
- **An example: The Famous Towers of Hanoi!**

Recursion



Towers of Hanoi

- The famous: “Towers of Hanoi” is a game to move a stack of n discs, while obeying certain, strict rules:
  - All n discs are of different sizes, residing on top of one another
  - A smaller disc always on top of a larger one
  - Goal is to move the whole tower from start, to goal, being allowed only three placement locations: start, goal and one additional buffer
  - But only move one disc at a time!
  - And never place a larger disc on top of a smaller!
- During various times, any disc may be placed on the start position, the goal, or the buffer
- But no other place!

Towers of Hanoi

```
#include <iostream.h>
#define MAX . . . some small integer < 32
void hanoi( int discs, char* start, char* goal, char* buff )
{ // hanoi
    . . . // see function body on next page
} // end hanoi

int main( void )
{ // main
   for( int discs = 1; discs <= MAX; discs++ ) {
      cout << ″ hanoi for " << discs << " discs" << endl;
      hanoi( discs, "start", "goal ", "buff " );
      cout << endl;
   } // end for
   return 0;
} // end main
```

Towers of Hanoi

```
#include <iostream.h>
#define MAX . . . some small integer << 32

void hanoi( int discs, char* start, char* goal, char* buff )
{ // hanoi
   if( discs > 0 ){
     hanoi( discs-1, start, buff, goal );
     cout << "move disc" << discs << "from" << start
          << "to" << goal << endl;
     hanoi( discs-1, buff, goal, start );
   } // end if
} // end hanoi
```

Towers of Hanoi

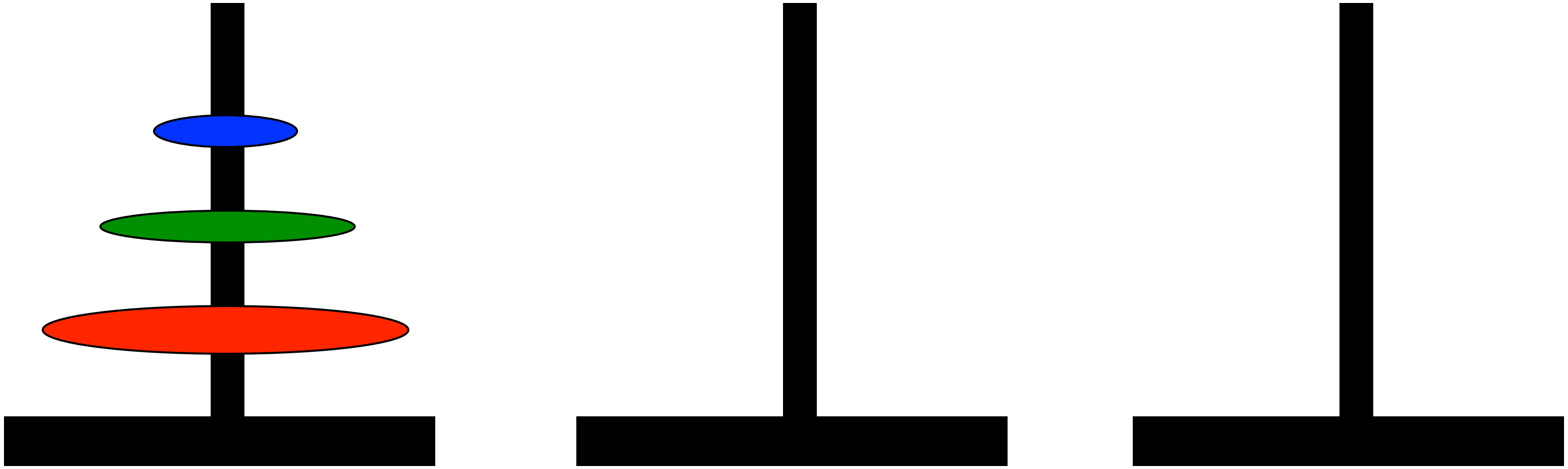
```
move disc 1 from start to goal    < For 1 disc

move disc 1 from start to buff    < For 2 discs
move disc 2 from start to goal
move disc 1 from buff  to goal

move disc 1 from start to goal    < For 3 discs
move disc 2 from start to buff
move disc 1 from goal  to buff
move disc 3 from start to goal
move disc 1 from buff  to start
move disc 2 from buff  to goal
move disc 1 from start to goal

move disc 1 from start to buff    < For 4 discs
move disc 2 from start to goal
move disc 1 from buff  to goal
move disc 3 from start to buff
move disc 1 from goal  to start
move disc 2 from goal  to buff
move disc 1 from start to buff
move disc 4 from start to goal
move disc 1 from buff  to goal
move disc 2 from buff  to start
move disc 1 from goal  to start
move disc 3 from buff  to goal
move disc 1 from start to buff
move disc 2 from start to goal
move disc 1 from buff  to goal
```

Towers of Hanoi

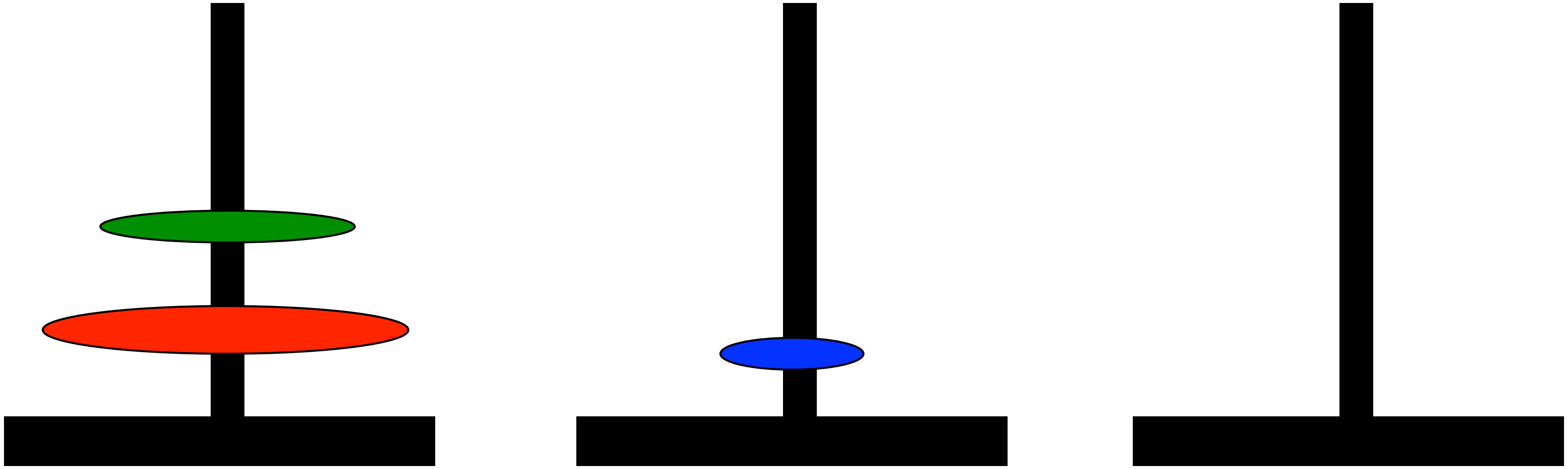
To be shown in much detail toward end of term, when we discus recursion in detail

Here just a playful introduction:

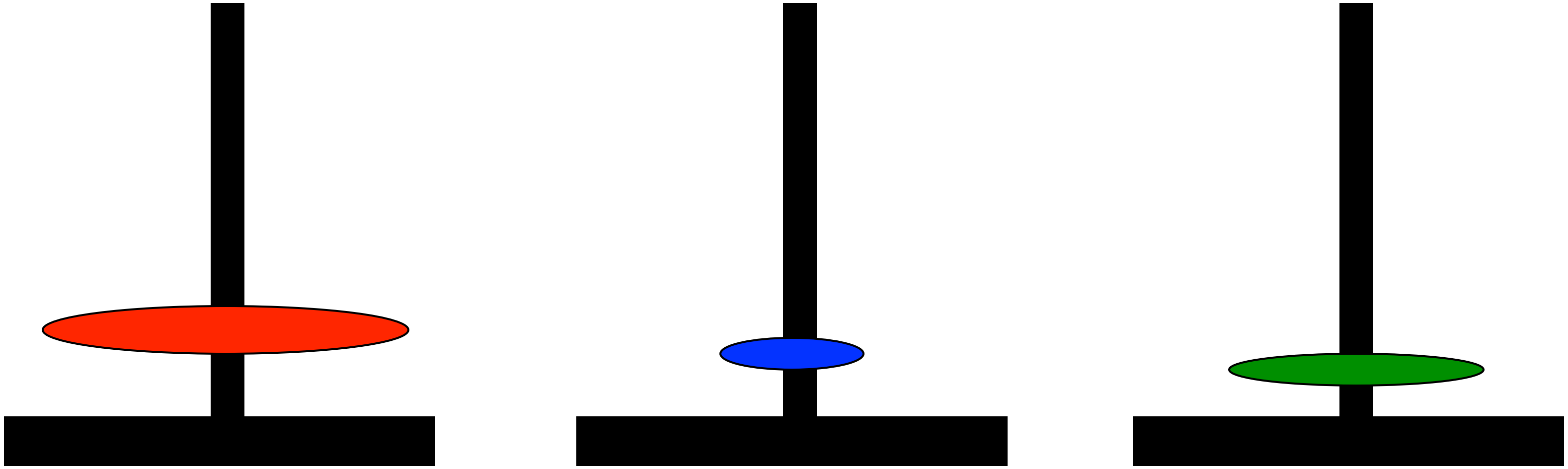
Towers of Hanoi



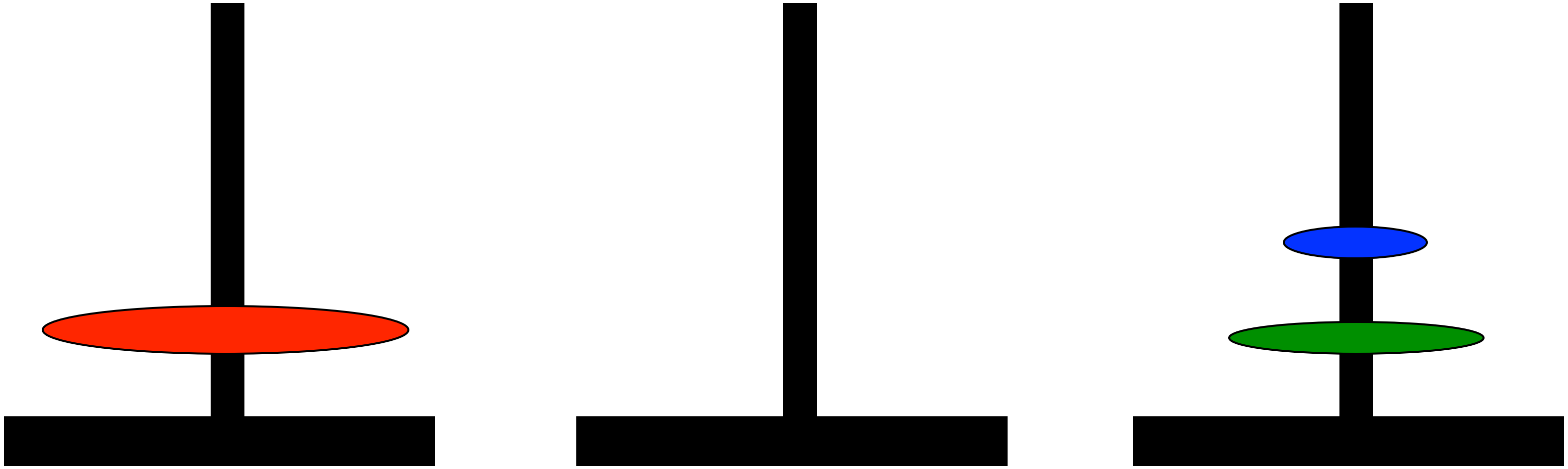
Towers of Hanoi



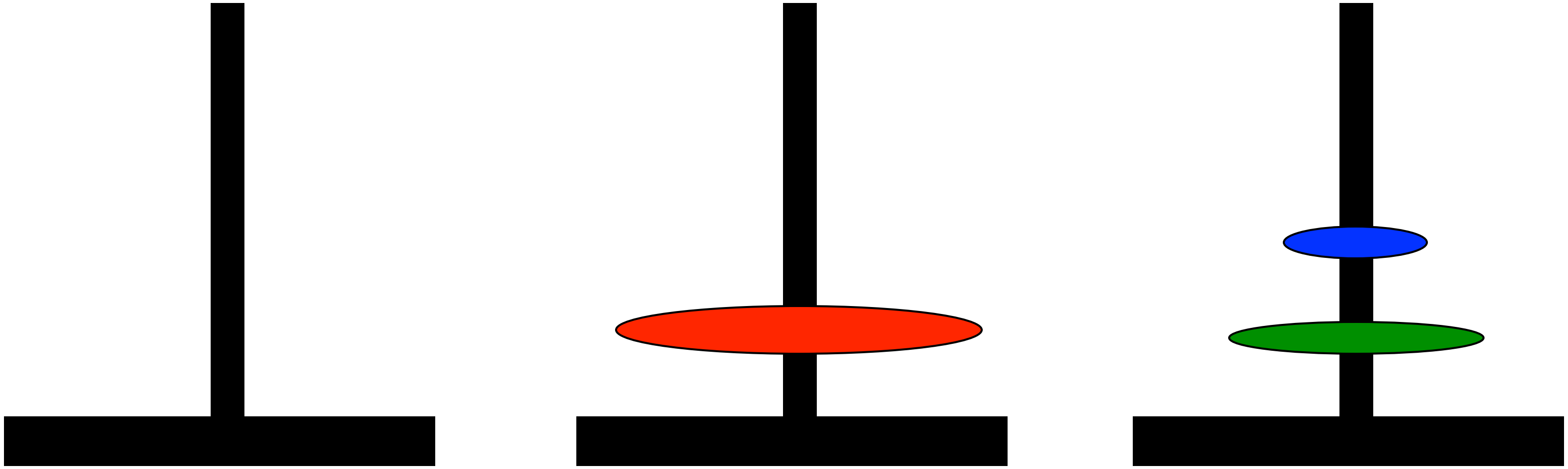
Towers of Hanoi



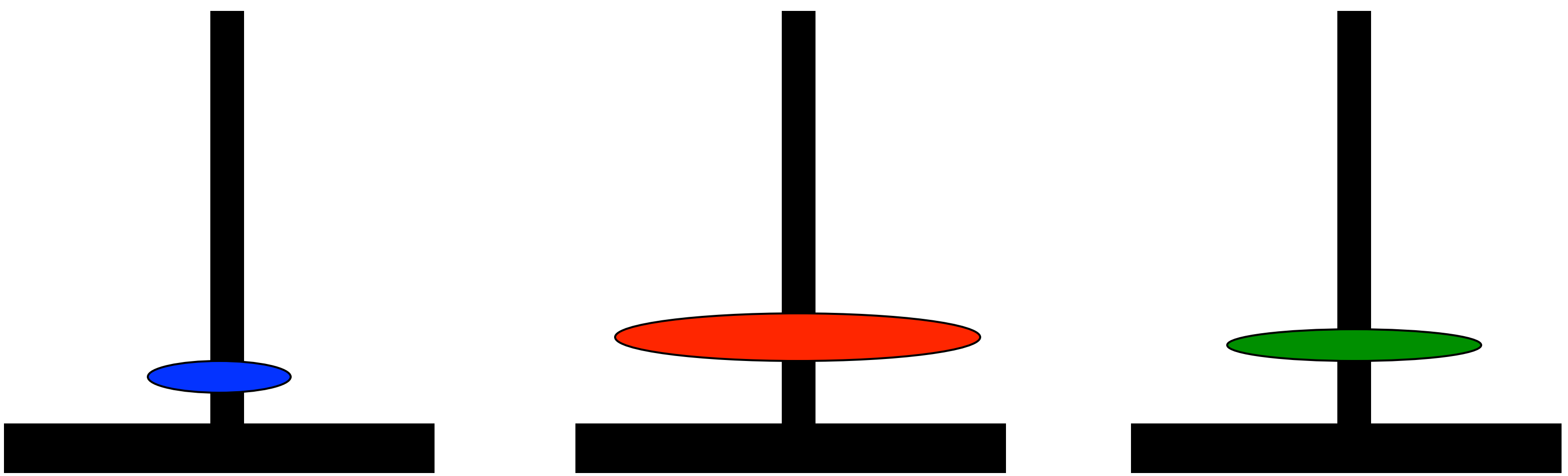
Towers of Hanoi



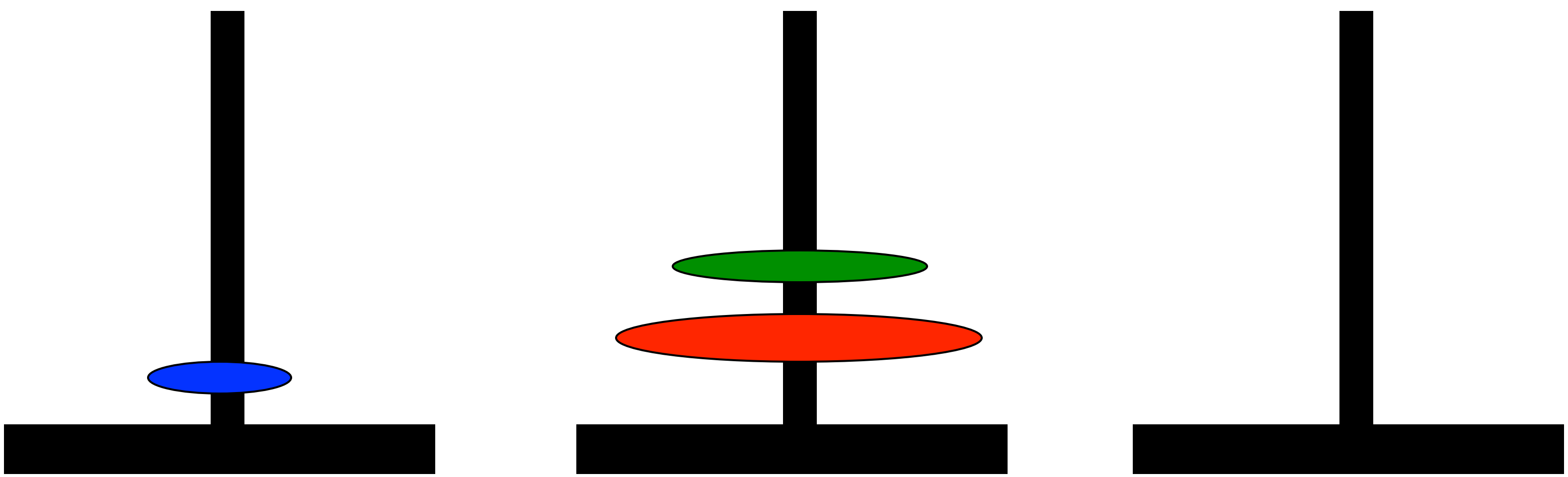
Towers of Hanoi



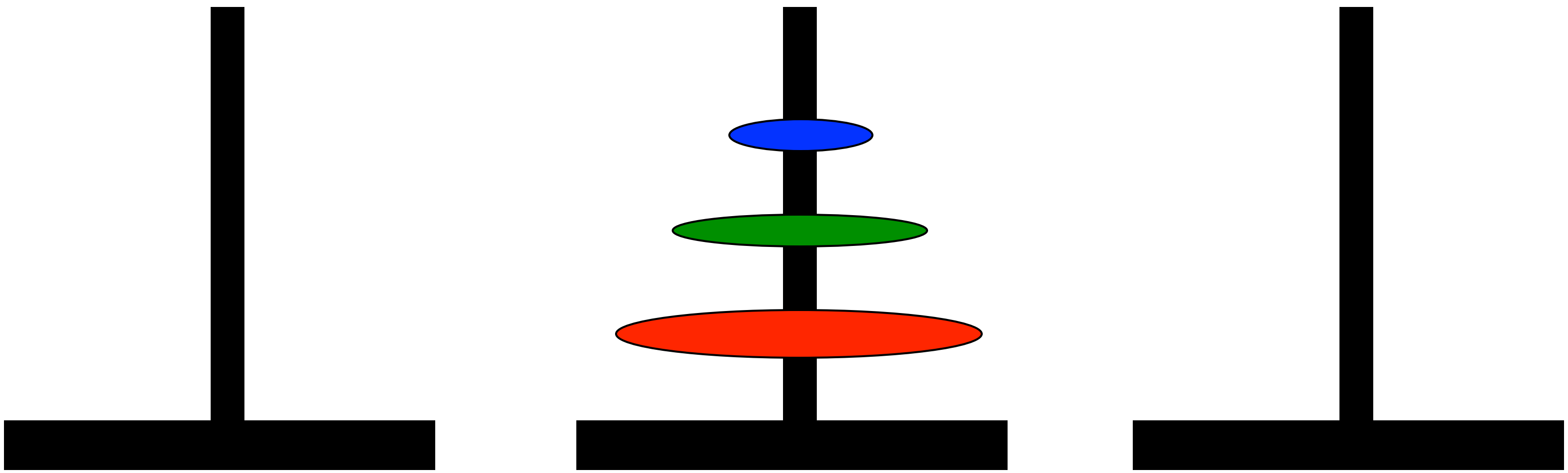
Towers of Hanoi



Towers of Hanoi



Towers of Hanoi



Summary

- Introduced Mathematical Induction, and elementary terms, such as set, power set
- An algorithm is recursive if it is partly defined in simpler versions of itself
- Equivalence of recursive programming solutions vs. iterative
- Game of the Towers of Hanoi

References

1. RSA Wiki 1:https://simple.wikipedia.org/wiki/RSA_algorithm
2. Game of Hanoi: https://en.wikipedia.org/wiki/Tower_of_Hanoi
3. Mathematical Induction Wiki: https://en.wikipedia.org/wiki/Mathematical_induction