# Lecture 1

# Introduction and Overview

COT 4420

Theory of Computation

Section 1.1

# Overview

- Understanding computation & computability
- Study finitary representations for languages and machines
- Understanding capabilities of abstract machines

# Algorithms and Procedures

- Procedure: finite sequence of instructions that can be carried out mechanically, say by a computer program.

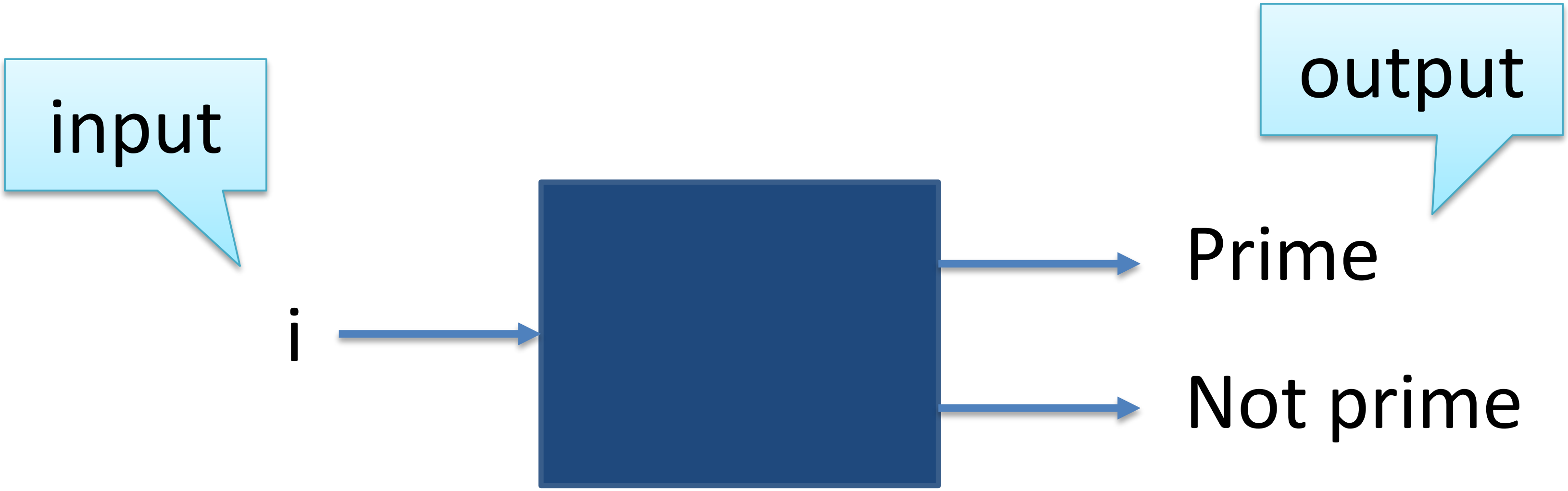
- Algorithm: a procedure that always halts is an algorithm.

# Example1

Example1: Determine if $i>1$ is a prime number

1. Set $j=2$
2. If $j >= i$ then halt; $i$ is a prime
3. If $i/j$ is an integer then halt; $i$ is not a prime
4. $j = j + 1$
5. Go to 2

# Example1




This is an **algorithm**: always halts and answers yes or no!

# Example2

Example2: Determine if a perfect number > $i$ exist

Note: A perfect number is a number that is equal to sum of its divisors (except for itself).

1. $j = i + 1$
2. If $j$ is perfect, halt.
3. $j = j + 1$
4. Go to 2

This is a **procedure**: It may never halt

# Mathematical preliminaries
## Sets

{a, b, c}, { 1, 2, 3, ..}, { $i$: $i$>0, $i$ is even}

A set $S_1$ is a **subset** of set S if every element of $S_1$ is also an element of S.

$$S_1 \subseteq S$$

$$\{a\} \subseteq \{a, b, c\}$$

$$\{a, b\} \subseteq \{a, b, c\}$$

# Mathematical preliminaries
## **Cardinality**

- How many elements are in a set?

The **cardinality** of a set is a measure of the size of the set and is denoted by |S|.

For finite sets: $S = \{a, b, c\}$ |S|=3

- How about the number of elements in $\mathbb{N}$ or $\mathbb{R}$?

$|\mathbb{N}| = \aleph_0$ (aleph-null)

# Mathematical preliminaries
## **Cardinality**

- Is the set of even numbers the same size as the set of natural numbers?

|Even|=?

**1 → 2**
**2 → 4**
**3 → 6**
**4 → 8**
**5 → 10**
**…**

We mapped *n* to *2n*

$|\text{Even}| = \aleph_0$

# Mathematical preliminaries
## **Cardinality**

- What about $|\mathbb{Z}|$=?

..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...

**8 6 4 2 0 1 3 5 7**

- A set S is called **countably infinite** iff $|S| = |\mathbb{N}|$

**Do all infinite sets have the same cardinality?**

# Mathematical preliminaries
## **Sets**

The **powerset** is a set of all subsets:

$$S = \{a, b, c\}$$

$$2^S = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Cardinality (size) of a set

$|S| = 3$

$|2^S| = 2^{|S|} = 2^3 = 8$

Why?

# Mathematical preliminaries
## Functions

A **function** is a rule that for every element of a set (domain) assigns an element of another set (range).

$$f : S_1 \rightarrow S_2$$

If the domain of $f$ is all of $S_1$, we say $f$ is a **total** function on $S_1$. Otherwise, $f$ is said to be a **partial** function.

# Mathematical preliminaries

## Relations

In a function, each element from the domain (input) is assigned to exactly one element from the range (output).

$$\{(1,2), (2,4), (3,6)\}$$

In a **relation**, there may be several elements from the range that is associated to one element in the domain.

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

A relation is a subset of $S_1 \times S_2$

# Mathematical preliminaries
## **Functions**

- A function is said to be **one-to-one**, if every element of the range corresponds to exactly one element of the domain.

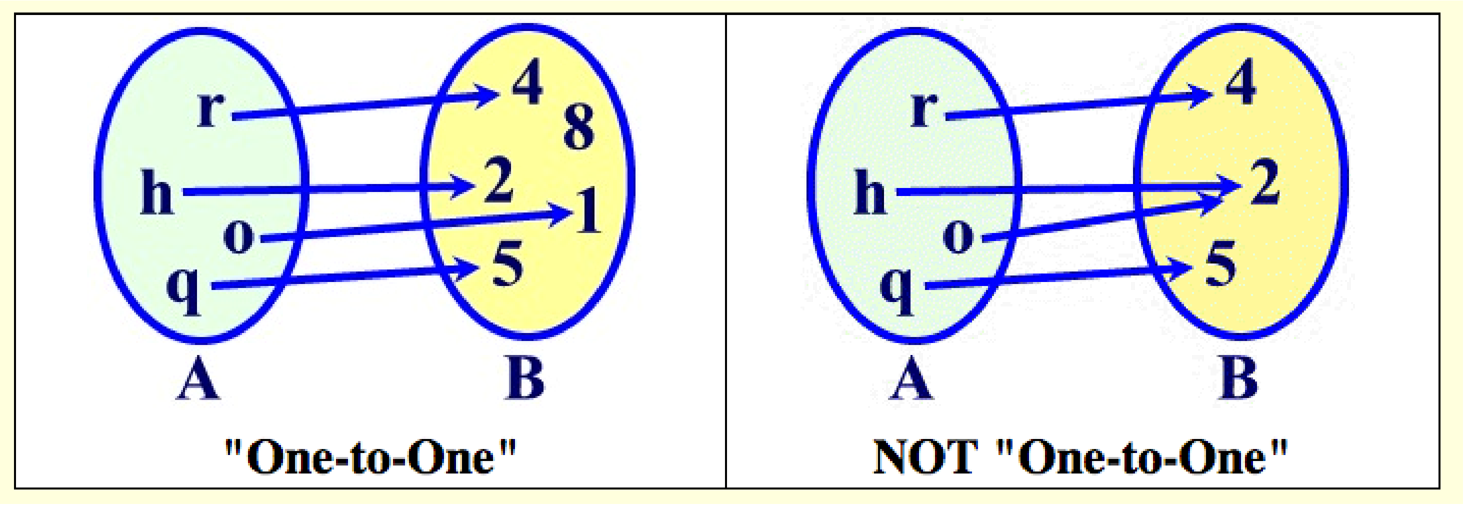



Image reference: http://www.regentsprep.org/Regents/math/algtrig/ATP5/OntoFunctions.htm

# Mathematical preliminaries
## **Functions**

- A function is said to be **onto**, if it covers all elements in the range.
- For all elements of the range, there is an element in the domain.

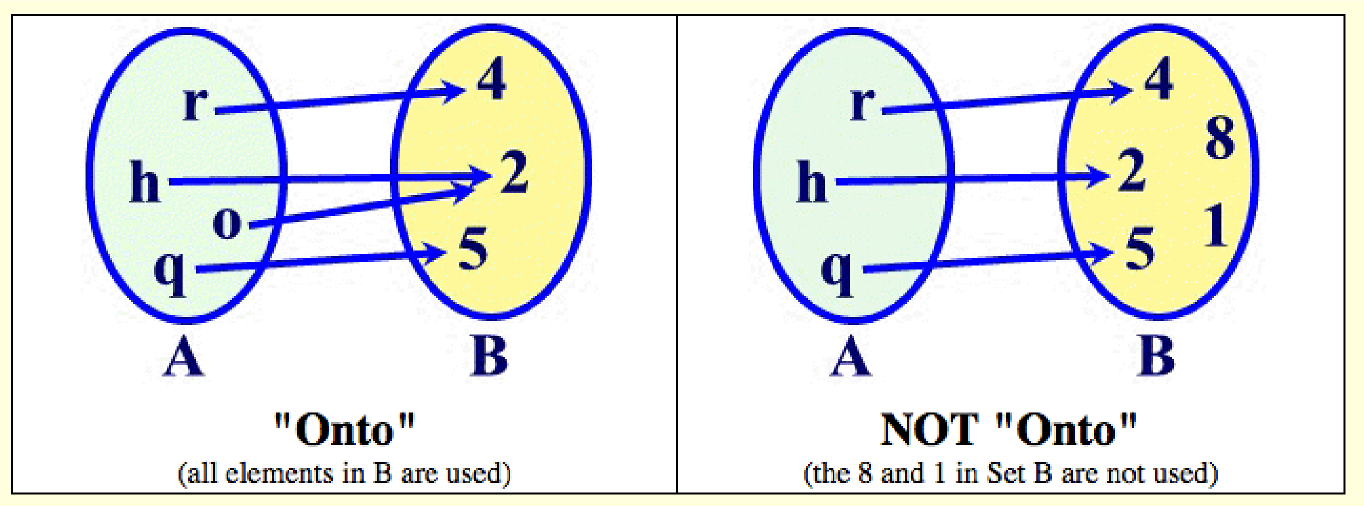



Image reference: http://www.regentsprep.org/Regents/math/algtrig/ATP5/OntoFunctions.htm

# Proof Techniques

## **Proof by induction**

1. Base case: We need to show that the given statement is true for the first natural number.

1. Inductive step: We need to prove that if the given statement is true for any number $\leq n$, it is also true for $n+1$.

# Proof by Induction

Example1:

prove that: $$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Base case: n=1 $$\sum_{i=1}^{1} i^2 = 1^2 = 1$$ trivially true

Inductive step: Assume it is true for ≤ n, prove true for n+1.

# Proof by Induction
# Example1

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

$$= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6}$$

$$= \frac{(n+1)\big(n(2n+1) + 6(n+1)\big)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

$$= \frac{(n+1)\big((n+1)+1\big)\big(2(n+1)+1\big)}{6}$$

# Proof by Induction
# Example2

Example2: Show that postages of $\geq 4$ can be achieved by using only 2-cent and 5-cent stamps.

Base case: $n = 4$ is true since you can use two 2-cent stamps.

Inductive step: Assume it is true for n. So n cent postage can be formed using only 2-cent and 5-cent stamps. Need to prove true for $n + 1$.

# Proof by Induction Example2

Note that for the case of n, either at least one 5-cent stamp must have been used or all 2-cent stamps were used..

Case1: if there is at least one 5-cent stamps, we can remove that stamp and replace it with three 2-cent stamps to form n+1.

Case2: If only 2-cent stamps were used, we remove two 2-cent stamps (note that n>4 so at least two 2-cent stamps must have been used in this case) and replace it with a 5-cent stamp to form n+1.

This proves the assertion fro n + 1.

# Proof Techniques
## **Proof by Contradiction**

We want to prove that statement P is true.

- We assume hypothetically that P is **not** true.
- If we arrive at a conclusion that we know is incorrect, we conclude that the initial assumption was false. So P must be true.

# Proof by Contradiction Example1

- Example1: Suppose $a \in Z$, If $a^2$ is even, then $a$ is even.
- Proof: We assume that the statement is not true. So $a^2$ is even, and $a$ is odd. Since $a$ is odd, there is an integer $k$ such that $a = 2k + 1$

$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \Rightarrow a^2$ is odd.

We know this is not true because it was our initial assumption that $a^2$ is even.

# Diagonalization Argument

- Prove that $|\mathbb{N}| < |\mathbb{R}|$

In order to prove this, we need to show that

$$|\mathbb{N}| \leq |\mathbb{R}| \text{ and } |\mathbb{N}| \neq |\mathbb{R}|$$

We can simply map every natural number to itself in $\mathbb{R}$. Therefore, $\mathbb{N}$ is no larger than $\mathbb{R}$.

Now we need to show that $|\mathbb{N}| \neq |\mathbb{R}|$.

# Diagonalization Argument

Suppose hypothetically that $|\mathbb{N}| = |\mathbb{R}|$

It means that $\mathbb{R}$ is countably infinite, and we should be able to count off all the real numbers.

Assume we have ordered the real numbers $r_0$, $r_1$, $r_2$, $r_3$, $r_4$, …

The idea is to find a real number *d* that isn't anywhere in this sequence, showing that we haven't counted off all the real numbers.

# Diagonalization Argument

- Note that every real number has an infinite representation:

  2 = 2.00000000000000

  π = 3.1415926535…..

- We define $r[0]$ to be the integer part of the real number and $r[n]$, $n>0$ to be the $n$th decimal digit

- We create $d$ such that $d[n]$ != $r_n[n]$

# Diagonalization Argument

$r_0 = 0.00000000...$

$r_1 = 1.02347612...$

$r_2 = 1.1098654.....$

$r_3 = 2.7610000000...$

$d = 1.219.....$

By contradiction we showed that $|\mathbb{N}| \neq |\mathbb{R}|$ and that $|\mathbb{N}| < |\mathbb{R}|$

# Uncountable sets

- A set S is called **uncountable** iff $|\mathbb{N}| < |S|$
- Note that the cardinality of the reals is uncountable.