# CS 207: Discrete Structures

Instructor : S. Akshay

July 21, 2015

Lecture 02 – Types of proofs, Mathematical Induction

# Logistics and recap

**Course material, references are being posted at**

- `http://www.cse.iitb.ac.in/~akshayss/teaching.html`
- Piazza has been set up. You will be getting the invites today.

# Logistics and recap

### Course material, references are being posted at

- `http://www.cse.iitb.ac.in/~akshayss/teaching.html`
- Piazza has been set up. You will be getting the invites today.

### Recap of last lecture

- What are discrete structures, course outline.
- Chapter 1: proofs and structures. Propositions, predicates.
- Theorems and proofs.

# Theorems and proofs

**A theorem is a proposition which can be shown true**

Prove the following theorems.

1. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$
2. If 6 is prime, then $6^2 = 30$.
3. Let $x$ be an integer. $x$ is even iff $x + x^2 - x^3$ is even.

4. There are infinitely many prime numbers.
5. There exist irrational numbers $x, y$ such that $x^y$ is rational.
6. For all $n \in \mathbb{N}$, $n! \leq n^n$.
7. There does not exist a (input-free) C-program which will always determine whether an arbitrary (input-free) C-program will halt.

# Theorems and proofs

## Contrapositive and converse

- The contrapositive of "if $A$ then $B$" is "if $\neg B$ then $\neg A$".
- A statement is logically equivalent to its contrapositive, i.e., it suffices to show one to imply the other.
- To show $A$ iff $B$, you have to show $A$ implies $B$ and conversely, $B$ implies $A$.
- Note the difference between contrapositive and converse.

# Proof by contradiction

**Theorem 4.: There are infinitely many primes.**

Proof by contradiction:

# Proof by contradiction

**Theorem 4.: There are infinitely many primes.**

Proof by contradiction:

- Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.

# Proof by contradiction

**Theorem 4.: There are infinitely many primes.**

Proof by contradiction:

- Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
- Let $k = (p_1 * p_2 * \ldots * p_r) + 1$. Then $k$ when divided by any $p_i$ has remainder 1. So $p_i \not| k$ for all $i \in \{1, \ldots, r\}$.

# Proof by contradiction

**Theorem 4.: There are infinitely many primes.**

Proof by contradiction:

- Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
- Let $k = (p_1 * p_2 * \ldots * p_r) + 1$. Then $k$ when divided by any $p_i$ has remainder 1. So $p_i \not| \; k$ for all $i \in \{1, \ldots, r\}$.
- But $k > 1$ and $k$ is not prime, so $k$ can be written as a product of primes (why?)

# Proof by contradiction

**Theorem 4.: There are infinitely many primes.**

Proof by contradiction:

- Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
- Let $k = (p_1 * p_2 * \ldots * p_r) + 1$. Then $k$ when divided by any $p_i$ has remainder 1. So $p_i \not| \, k$ for all $i \in \{1, \ldots, r\}$.
- But $k > 1$ and $k$ is not prime, so $k$ can be written as a product of primes (why?)
- Fundamental theorem of arithmetic: any natural number $> 1$ can be written as a unique product of primes.

# Proof by contradiction

**Theorem 4.: There are infinitely many primes.**

Proof by contradiction:

- Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
- Let $k = (p_1 * p_2 * \ldots * p_r) + 1$. Then $k$ when divided by any $p_i$ has remainder 1. So $p_i \not| \, k$ for all $i \in \{1, \ldots, r\}$.
- But $k > 1$ and $k$ is not prime, so $k$ can be written as a product of primes (why?)
- Fundamental theorem of arithmetic: any natural number $> 1$ can be written as a unique product of primes.
- Now let $p | k$. But $p \notin \{p_1, \ldots, p_r\}$, so this is a contradiction.

# A Non-constructive proof

**Theorem 5.:** There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

# A Non-constructive proof

**Theorem 5.:** There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.

# A Non-constructive proof

**Theorem 5.:** There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If $z$ is rational, we are done (why?)

# A Non-constructive proof

Theorem 5.: There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If $z$ is rational, we are done (why?)
- Case 2: Else $z$ is irrational.

# A Non-constructive proof

**Theorem 5.:** There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If $z$ is rational, we are done (why?)
- Case 2: Else $z$ is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.

# A Non-constructive proof

**Theorem 5.:** There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If $z$ is rational, we are done (why?)
- Case 2: Else $z$ is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.
  - Thus we have found two irrationals $x = z, y = \sqrt{2}$ such that $x^y = 2$ is rational. $\square$

# A Non-constructive proof

**Theorem 5.:** There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If $z$ is rational, we are done (why?)
- Case 2: Else $z$ is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.
  - Thus we have found two irrationals $x = z, y = \sqrt{2}$ such that $x^y = 2$ is rational. $\square$

Indeed, note that the above proof is not constructive!

# A Non-constructive proof

**Theorem 5.:** There exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If $z$ is rational, we are done (why?)
- Case 2: Else $z$ is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.
  - Thus we have found two irrationals $x = z, y = \sqrt{2}$ such that $x^y = 2$ is rational. $\square$

Indeed, note that the above proof is not constructive!

(H.W): Post a constructive proof of this theorem on piazza.

# Types of proofs

1. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
2. If 6 is prime, then $6^2 = 30$.
3. $x$ is an even integer iff $x + x^2 - x^3$ is even.
4. There are infinitely many prime numbers.
5. There exist irrational numbers $x, y$ such that $x^y$ is rational.
6. For all $n \in \mathbb{N}$, $n! \leq n^n$.
7. There does not exist a (input-free) C-program which will always determine whether an arbitrary (input-free) C-program will halt.

# Types of proofs

1. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
   – Direct proof
2. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof
3. $x$ is an even integer iff $x + x^2 - x^3$ is even.
   – Both directions, by contrapositive $(A \to B = \neg B \to \neg A)$
4. There are infinitely many prime numbers.
   – Proof by contradiction
5. There exist irrational numbers $x, y$ such that $x^y$ is rational.
   – Non-constructive proof
6. For all $n \in \mathbb{N}$, $n! \leq n^n$.
7. There does not exist a (input-free) C-program which will always determine whether an arbitrary (input-free) C-program will halt.

# Types of proofs

1. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
   – Direct proof
2. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof
3. $x$ is an even integer iff $x + x^2 - x^3$ is even.
   – Both directions, by contrapositive $(A \to B = \neg B \to \neg A)$
4. There are infinitely many prime numbers.
   – Proof by contradiction
5. There exist irrational numbers $x, y$ such that $x^y$ is rational.
   – Non-constructive proof
6. For all $n \in \mathbb{N}$, $n! \leq n^n$. – next!
7. There does not exist a (input-free) C-program which will always determine whether an arbitrary (input-free) C-program will halt.

# Theorems and proofs

**What are the common/significant elements of the proofs?**

- Rules of inference: Logic, e.g., if $p$ is true, and $p$ implies $q$, then $q$ is true.)
- Axioms: Peano's axioms, Euclid's axioms.
- Strategies: vacuous, direct, case-by-case, contrapositive, contradiction, constructive, non-constructive.

# Theorems and proofs

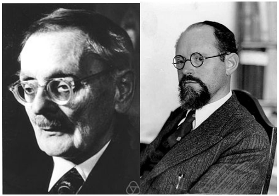
**What are the common/significant elements of the proofs?**

- Rules of inference: Logic, e.g., if $p$ is true, and $p$ implies $q$, then $q$ is true.)
- Axioms: Peano's axioms, Euclid's axioms.
- Strategies: vacuous, direct, case-by-case, contrapositive, contradiction, constructive, non-constructive.
  - Role of counter-examples: Prove or disprove: For all $x \in \mathbb{N}$, $x^2 + x + 41$ is prime.

# Axioms

(a) Euclid

(b) G. Peano



(c) Zermelo-Fraenkel

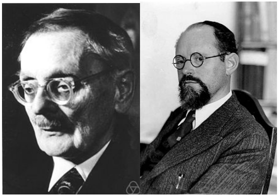
(a) Euclid's axioms for geometry in 300 BCE.

(b) Peano's axioms for natural numbers in 1889.

# Axioms

(a) Euclid

(b) G. Peano



(c) Zermelo-Fraenkel

(a) Euclid's axioms for geometry in 300 BCE.
(b) Peano's axioms for natural numbers in 1889.
(c) Zermelo-Fraenkel and Choice axioms (ZFC) are a small set of axioms from which most of mathematics can be inferred.

  - But proving even 2+2=4 requires > 20000 lines of proof!

- In this course, we will assume axioms, mostly from high school math (distributivity of numbers etc.).

# Introducing the world of Mathematical Induction

## Induction (Axiom)

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction Step)

  then $P(n)$ is true for all $n \in \mathbb{N}$.

# Introducing the world of Mathematical Induction

## Induction (Axiom)

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction Step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

## Theorem 6.: For all integers $n > 1$, $n! \leq n^n$

Proof by induction:

# Introducing the world of Mathematical Induction

## Induction (Axiom)

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction Step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

## Theorem 6.: For all integers $n > 1$, $n! \leq n^n$

Proof by induction:

- Base case: For $n = 1$, $1! = 1^1$, so statement is true.

# Introducing the world of Mathematical Induction

## Induction (Axiom)

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction Step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

## Theorem 6.: For all integers $n > 1$, $n! \leq n^n$

Proof by induction:

- Base case: For $n = 1$, $1! = 1^1$, so statement is true.
- Induction Hypothesis: Suppose for some $n = k \geq 1$, $k! \leq k^k$

# Introducing the world of Mathematical Induction

**Induction (Axiom)**

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction Step)

  then $P(n)$ is true for all $n \in \mathbb{N}$.

**Theorem 6.: For all integers $n > 1$, $n! \leq n^n$**

Proof by induction:

- Base case: For $n = 1$, $1! = 1^1$, so statement is true.
- Induction Hypothesis: Suppose for some $n = k \geq 1$, $k! \leq k^k$
- Then we have the induction step:

$$(k+1)! = k! \cdot (k+1) \leq k^k(k+1) \text{(by Induction Hypothesis)}$$
$$< (k+1)^k \cdot (k+1) = (k+1)^{(k+1)} \quad \square$$

# Examples by induction (H.W)

1. Summations:
   1.1 $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.
   1.2 $1^2 - 2^2 + 3^2 - \cdots + (-1)^n n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$

# Examples by induction (H.W)

1. Summations: For every positive integer $n$,
   1.1 $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.
   1.2 $1^2 - 2^2 + 3^2 - \cdots + (-1)^n n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$

# Examples by induction (H.W)

1. Summations: For every positive integer $n$,
   1.1 $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.
   1.2 $1^2 - 2^2 + 3^2 - \cdots + (-1)^n n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$
2. Inequalities
   2.1 If $h > -1$, then $1 + nh \leq (1 + h)^n$ for all non-negative integers $n$.
3. Divisibility
   3.1 6 divides $n^3 - n$ when $n$ is a non-negative integer.
   3.2 21 divides $4^{n+1} - 5^{n-1}$ whenever $n$ is positive integer.
4. Many more... including correctness/optimality of algorithms.

# Examples by induction (H.W)

1. Summations: For every positive integer $n$,
   1.1 $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.
   1.2 $1^2 - 2^2 + 3^2 - \cdots + (-1)^n n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$
2. Inequalities
   2.1 If $h > -1$, then $1 + nh \leq (1+h)^n$ for all non-negative integers $n$.
3. Divisibility
   3.1 6 divides $n^3 - n$ when $n$ is a non-negative integer.
   3.2 21 divides $4^{n+1} - 5^{n-1}$ whenever $n$ is positive integer.
4. Many more... including correctness/optimality of algorithms.

– "Proof technique" rather than a "Solution technique" as it requires a good guess of the answer.

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n-1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction:

- Base case: if $n = 0$, $f(a, 0) = 1 = a^0$ for all non-zero real $a$.

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction:

- Base case: if $n = 0$, $f(a, 0) = 1 = a^0$ for all non-zero real $a$.
- Induction step: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.
- Now for $n = k + 1$, $f(a, k + 1) = a \cdot f(a, k) = a \cdot a^k = a^{k+1}$ (by Induction Hyp).
- Thus, by induction for all non-negative integers $n$, the algorithm above computes $f(a, n) = a^n$. $\square$

# Interesting fallacy in using induction!

**Conjecture:** All horses have the same colour.

"Proof" by induction:

- The case with one horse is trivial.
- Assume for $n = k$ and now we have $k+1$ horses, say $1, \ldots, k+1$.
  - (A) First, consider horses $1, \ldots, k$. By induction hypothesis, they have same color.
  - (B) Next, consider horses $2, \ldots, k+1$. By induction hypothesis, they have same color.
  - (C) Therefore, 1 has same color as 2 (by A) and 2 has same color as $k+1$ (by B), implies all $k+1$ have same color.
- Thus all collections of horses have same color. $\square$

Where is the bug?

# What is the basis for induction

**Axiom (Well Ordering Principle)**

Every nonempty set of non-negative integers has a smallest element.

# What is the basis for induction

**Axiom (Well Ordering Principle)**

Every nonempty set of non-negative integers has a smallest element. Does this seem familiar? Obvious? What about for rationals?!

# What is the basis for induction

**Axiom (Well Ordering Principle)**

Every nonempty set of non-negative integers has a smallest element.

**Axiom (Induction)**

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contraction:

- Suppose, $P(0)$ is true and for each $n \geq 0$, and $P(n) \implies P(n+1)$ but, $P(n)$ is not true for all non-negative integers.

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

- Suppose, $P(0)$ is true and for each $n \geq 0$, and $P(n) \implies P(n+1)$ but, $P(n)$ is not true for all non-negative integers.
- Consider $S = \{i \in \mathbb{N} \mid P(i) \text{ is false }\}$.
- $S$ is a non-empty set of non-negative integers, hence by WOP, it has a smallest element, say $i_0$.
- $i_0 \neq 0$. Also $i_0 - 1 \notin S$, so $P(i_0 - 1)$ is true. But then for $n = i_0 - 1$, we contradict $P(i_0 - 1) \implies P(i_0)$. $\square$

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

- Suppose, $P(0)$ is true and for each $n \geq 0$, and $P(n) \implies P(n+1)$ but, $P(n)$ is not true for all non-negative integers.
- Consider $S = \{i \in \mathbb{N} \mid P(i) \text{ is false } \}$.
- $S$ is a non-empty set of non-negative integers, hence by WOP, it has a smallest element, say $i_0$.
- $i_0 \neq 0$. Also $i_0 - 1 \notin S$, so $P(i_0 - 1)$ is true. But then for $n = i_0 - 1$, we contradict $P(i_0 - 1) \implies P(i_0)$. $\square$

**Theorem: WOP iff Induction**

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

- Suppose, $P(0)$ is true and for each $n \geq 0$, and $P(n) \implies P(n+1)$ but, $P(n)$ is not true for all non-negative integers.
- Consider $S = \{i \in \mathbb{N} \mid P(i) \text{ is false } \}$.
- $S$ is a non-empty set of non-negative integers, hence by WOP, it has a smallest element, say $i_0$.
- $i_0 \neq 0$. Also $i_0 - 1 \notin S$, so $P(i_0 - 1)$ is true. But then for $n = i_0 - 1$, we contradict $P(i_0 - 1) \implies P(i_0)$. $\square$

**Theorem: WOP iff Induction**

(H.W) Prove the reverse direction.

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

**Theorem:** Any integer $> 1$ is either a prime or can be written as a product of primes

- Prove this theorem by either directly using WOP or by induction.