CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Aug 05, 2024

Lecture 04 – Induction

Logistics and recap

Course material, references are being posted at

- `http://www.cse.iitb.ac.in/~akshayss/teaching.html`

Logistics and recap

Course material, references are being posted at

- http://www.cse.iitb.ac.in/~akshayss/teaching.html
- Problem Sheet 1 is on Piazza
  - https://piazza.com/iit_bombay/fall2024/cs105

Logistics and recap

Course material, references are being posted at

- http://www.cse.iitb.ac.in/~akshayss/teaching.html
- Problem Sheet 1 is on Piazza
  - https://piazza.com/iit_bombay/fall2024/cs105

Recap of three lectures

- What are discrete structures?
- Course outline
- Chapter 1: Proofs and structures
  - Propositions: statements that can be assigned a truth value
  - Predicates: propositions with variables
  - Quantifiers
  - Theorems and different types of proofs

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$

2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.

3. If 6 is prime, then $6^2 = 30$.
4. x is an even integer iff $x + x^2 - x^3$ is even.

5. There are infinitely many prime numbers.

6. There exist irrational numbers x, y such that x^y is rational.

7. For all $n \in \mathbb{N}$, $n! \leq n^n$.
8. There does not exist a (input-free) program which will always determine whether an arbitrary (input-free) program will halt.

Types of proofs

1. $\neg(p \land q)$ is logically equivalent to $\neg p \lor \neg q$

   – By truth tables
2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.

   – Direct proof
3. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof
4. x is an even integer iff $x + x^2 - x^3$ is even.

   – Both directions, by contrapositive $(A \to B = \neg B \to \neg A)$
5. There are infinitely many prime numbers.

   – Proof by contradiction
6. There exist irrational numbers x, y such that x^y is rational.

   – Non-constructive proof
7. For all $n \in \mathbb{N}$, $n! \leq n^n$.
8. There does not exist a (input-free) program which will always determine whether an arbitrary (input-free) program will halt.

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$

   – By truth tables

2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.

   – Direct proof

3. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof

4. x is an even integer iff $x + x^2 - x^3$ is even.

   – Both directions, by contrapositive ($A \to B = \neg B \to \neg A$)

5. There are infinitely many prime numbers.

   – Proof by contradiction

6. There exist irrational numbers x, y such that x^y is rational.

   – Non-constructive proof

7. For all $n \in \mathbb{N}$, $n! \leq n^n$. – next!

8. There does not exist a (input-free) program which will always determine whether an arbitrary (input-free) program will halt.

Theorems and proofs

What are the common/significant elements of the proofs?

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.
  - if p is true, then $p \vee q$ is true.
  - if p is true and q is true, then $p \wedge q$ is true.
  - if p implies q and q implies r, then p implies r.
  - if $p \vee q$ is true and p is false, then q is true.

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.
  - if p is true, then $p \vee q$ is true.
  - if p is true and q is true, then $p \wedge q$ is true.
  - if p implies q and q implies r, then p implies r.
  - if $p \vee q$ is true and p is false, then q is true.
- 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.
  - if p is true, then $p \vee q$ is true.
  - if p is true and q is true, then $p \wedge q$ is true.
  - if p implies q and q implies r, then p implies r.
  - if $p \vee q$ is true and p is false, then q is true.
- 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.

Theorems and proofs

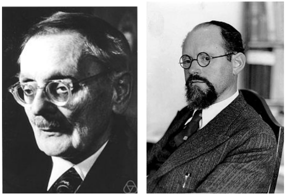
What are the common/significant elements of the proofs?

- Rules of inference: Logic, e.g.,
  - if p is true, and p implies q, then q is true.
  - if p is true, then $p \vee q$ is true.
  - if p is true and q is true, then $p \wedge q$ is true.
  - if p implies q and q implies r, then p implies r.
  - if $p \vee q$ is true and p is false, then q is true.
- 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: Peano's axioms, Euclid's axioms.

Axioms

(a) Euclid

(b) G. Peano



(c) Zermelo-Fraenkel

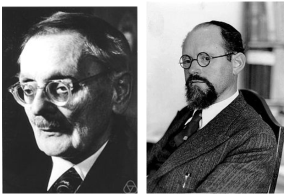
(a) Euclid's axioms for geometry in 300 BCE.

(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 7.: For all integers $n > 1$, $n! < n^n$

Proof by induction: we will show for all $n \geq 2$, $n! < n^n$

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 7.: For all integers $n > 1$, $n! < n^n$

Proof by induction: we will show for all $n \geq 2$, $n! < n^n$

1. Base case For $n = 2$, $2! = 2 \leq 4 = 2^2$, so Base Case 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 7.: For all integers $n > 1$, $n! < n^n$

Proof by induction: we will show for all $n \geq 2$, $n! < n^n$

1. Base case For $n = 2$, $2! = 2 \leq 4 = 2^2$, so Base Case is true.
2. Induction Hypothesis: Assume, for some $n = k \geq 2$, $k! < k^k$

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 7.: For all integers $n > 1$, $n! < n^n$

Proof by induction: we will show for all $n \geq 2$, $n! < n^n$

1. Base case For $n = 2$, $2! = 2 \leq 4 = 2^2$, so Base Case is true.
2. Induction Hypothesis: Assume, for some $n = k \geq 2$, $k! < k^k$
3. Induction step: To show: $(k+1)! \leq (k+1)^{(k+1)}$

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 7.: For all integers $n > 1$, $n! < n^n$

Proof by induction: we will show for all $n \geq 2$, $n! < n^n$

1. Base case For $n = 2$, $2! = 2 \leq 4 = 2^2$, so Base Case is true.
2. Induction Hypothesis: Assume, for some $n = k \geq 2$, $k! < k^k$
3. Induction step: To show: $(k+1)! \leq (k+1)^{(k+1)}$

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

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 7.: For all integers $n > 1$, $n! < n^n$

Proof by induction: we will show for all $n \geq 2$, $n! < n^n$

1. Base case For $n = 2$, $2! = 2 \leq 4 = 2^2$, so Base Case is true.
2. Induction Hypothesis: Assume, for some $n = k \geq 2$, $k! < k^k$
3. Induction step: To show: $(k+1)! \leq (k+1)^{(k+1)}$

$$\begin{aligned}(k+1)! = k! \cdot (k+1) &\leq k^k(k+1) \text{ (by Induction Hypothesis)} \\ &< (k+1)^k \cdot (k+1) = (k+1)^{(k+1)}\end{aligned}$$

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 7.: For all integers $n > 1$, $n! < n^n$

Proof by induction: we will show for all $n \geq 2$, $n! < n^n$

1. Base case For $n = 2$, $2! = 2 \leq 4 = 2^2$, so Base Case is true.
2. Induction Hypothesis: Assume, for some $n = k \geq 2$, $k! < k^k$
3. Induction step: To show: $(k+1)! \leq (k+1)^{(k+1)}$

$$\begin{aligned} (k+1)! = k! \cdot (k+1) &\leq k^k(k+1) \text{ (by Induction Hypothesis)} \\ &< (k+1)^k \cdot (k+1) = (k+1)^{(k+1)} \end{aligned}$$

4. Hence by induction, we conclude that for all $n \geq 2$, $n! < n^n$.

Examples by induction (H.W)

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

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 $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$

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 $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$
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 $4^{n+1} + 5^{2n-1}$ 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 $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}\frac{n(n+1)}{2}$
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 $4^{n+1} + 5^{2n-1}$ 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.

Interesting fallacy in using induction!

Conjecture: All horses have the same colour.

"Proof" by induction on number of horses:

1. Base Case ($n = 1$) The case with one horse is trivial.
2. Induction Hypothesis Assume for $n = k \geq 1$, i.e., any set of $k(\geq 1)$ horses has same color.
3. Induction Step We want to show any set of $k + 1$ horses have same color. Consider such a set, 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.
4. Thus, by induction, we conclude that for all $n \geq 1$, any set of n horses has the same color. $\square$

Where is the bug?