CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Aug 05, 2025

Lecture 03 – Theorems, types of proofs

Theorems and proofs

A theorem is a proposition which can be shown true

Classwork: Prove the following theorems.

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. For all $x \in \mathbb{Z}$, x is an even 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 integers $n > 1$, $n! < n^n$.
8. There does not exist a program which will always determine whether an arbitrary (input-free) program will terminate.

Theorems and proofs

Recall: 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.
- i.e., $p \to q$ is logically equivalent to $\neg q \to \neg p$
- The converse of "if A then B" is "if B then A".
- Common mistake: Contrapositive not the same as converse!

To show "A iff B", you must show two things:

1. A implies B and
2. its converse, B implies A OR $\neg A$ implies $\neg B$.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)
  1. We will show contrapositive! i.e., x is not even $\implies$ $x + x^2 - x^3$ is not even, i.e., x is odd $\implies$ $x + x^2 - x^3$ is odd.
  2. Let $x \in \mathbb{Z}$ be odd, i.e., $x = 2k + 1$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3$ is odd! (check this!). Hence proved.

$\square$

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

1. Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
2. Let $k = (p_1 * p_2 * \ldots * p_r) + 1$.
3. Then k when divided by any p_i has remainder 1. So none of the p_i's divide k.
4. But $k > 1$ and k is not prime (since $k > p_r$), 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.
5. Now take any prime p in this product, then, p divides k. So, by 3. above, $p \notin \{p_1, \ldots, p_r\}$.
6. This contradicts 1. since we had assumed that $\{p_1, \ldots p_r\}$ was the set of all primes. $\square$

A Non-constructive proof

Theorem 6.: 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 $x = z = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ 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. $\neg(p \wedge q)$ 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 integers $n > 1$, $n! < n^n$. – next!

8. There does not exist a 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?

- 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.

(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 $n \in \mathbb{N}$.

Theorem 6.: 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 $n = 2$, $2! = 2 < 4 = 2^2$, so Base Case is true.
2. Induction Hypothesis: Assume, for some $n = k \geq 2$, $k! < k^k$
3. Induction step: To show: $(k+1)! < (k+1)^{(k+1)}$

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

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

Examples by induction (H.W)

1. Summations: 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 $1, \dots, k + 1$.
   (A) First, consider horses $1, \dots, k$. By induction hypothesis, they have same color.
   (B) Next, consider horses $2, \dots, k + 1$. 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?