Lecture 1: Proofs

Date: **29-Nov-2021**

CS1010: Discrete Mathematics

IIT Hyderabad, Odd Semester (2021)

Welcome to CS1010: Discrete Math for CS

- This class is intended for:
  - First year CS / First or Second year of other relevant disciplines

- What you will learn:
  - Understanding the fundamentals of mathematical logic and reasoning, especially relevant for CS
  - *Structures* of discrete objects
  - Combinatorics and counting, some probability
  - Abstract algebra, other applications

- Order may be interwoven depending on progress of lectures; topics may be interdependent.

Course Logistics

- Instructor: Rakesh Venkat

- Lectures in *Slot **P***:
  - Mon (2:30pm - 4:00pm)
  - Thurs (4:00pm – 5:30pm)

- Teaching Assistants:
  - (Will be updated soon!)

- Office hours (to meet me regarding any course-related concerns):
  - Email me; if needed we can meet (online) after fixing a time over email

Online classes

- Treat it like a normal class (as much as is possible!)
  - Take notes, attend classes, stick to the schedule
  - Avoid procrastination on tutorials, readings
  - Do not hesitate to ask questions or interact in class; will help everyone (including me!).
  - I will follow a blackboard-style teaching for the most part
- **Academic Honesty** is non-negotiable. Please read the CSE Department's anti-plagiarism policy at: https://cse.iith.ac.in/academics/plagiarism-policy.html
- **Plagiarism** detected would be a 0 in the quiz + grade penalty. A repeat offence will attract greater penalty (up to F –grade).
  - If you are unsure if what you are doing is plagiarism, ***ask** the instructor (me).*

Evaluation

- 4 Quizzes at roughly equal intervals throughout the course

Quiz #	Marks	Dates (Likely)
Quiz 0	0	13 Dec
Quiz 1	15	20 Dec
Quiz 2	20	17 Jan
Quiz 3	15	14 Feb
Quiz 4	25	14 Mar
Total	75	

Other	Remark
15 marks	Either online or offline weekly questions
10 marks	Homeworks /Writeup

Topic for writeup will be assigned at end of every unit, on a related topic not covered in class.

- Attending Quiz 0 is compulsory.

- Objective weekly/bi-weekly exercises are meant to test basic understanding

- Missed quiz: No make-up, except for genuine medical reasons.

Platforms for Online classes

- **Google Classroom** for announcements, discussions and notes; you will receive an invite soon.

- **MS Teams** link for live lectures. **Youtube** for uploaded recordings.

- **SAFE app + MS Teams** for Conducting quizzes.
  - Quizzes will require Video Proctoring. TAs will hold a class + Quiz 0.

- **Possible use:** Gradescope for viewing corrected homeworks.

Textbooks for the course

- "Mathematics for Computer Science" by Eric Lehman, F. Thomson Leighton, Albert R. Meyer; available online

- “Discrete Mathematics and Its Applications”, by Kenneth Rosen. Edition 7.

- Lots of resources available online (e.g. MIT Open Courseware 6.042J is based on the Lehman-Leighton-Meyer book)

Proofs, Mathematical Reasoning, Structures

Today

- Proofs, Importance of Proofs

- Types of Proofs

- Some points for writing a *good* proof

- Reference: Chapter 1 of [LLM]

What is a proof

- Prove that it rained today.

It rained today. → Statement that is either True or False is a $\boxed{\text{Proposition}}$.

What is a proof.

more precise by stating the place.

- $1+1=2$.

- Proposition : $p(n) := n^2+n+41$. → claim that $p(n)$ is a prime for all $n \in \mathbb{N}$.

$\triangleq$ or others also used (Definition)

for all → $\forall$.

$\in$ → "in".

$\mathbb{N}$ → set of $\{1, 2, \cdots\}$.

Proposition: $p(n) = n^2 + n + 41$. is prime $\forall n \in \mathbb{N}$.

Proof: False. $p(41) = 41^2 + 41 + 41$ is

$$p(40) = 40^2 + 40 + 41 = 40(40+1) + 41$$

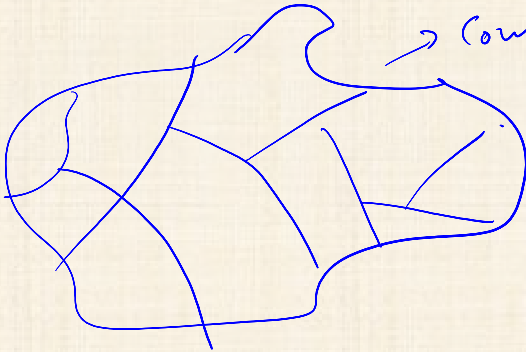
$$\underbrace{p(1),\ p(2)\ \ldots\ p(39)}$$ are all prime.

Euler: $a^4 + b^4 + c^4 = d^4$ has no solution over $\mathbb{N}$.

218 years later. $\left\{ a = 95800,\ b = 217519,\ c = 414560,\ d = 422481 \right\}$

1630 Fermat $\underline{x^n + y^n = z^n}$. There do not exist $x, y, z \in \mathbb{N}$ for some $n > 2$ that the above is true. Proved in 1994 by Wiles.

4-Color theorem.



→ Country.

→ Proof using a computer!
↓
Check various cases.

(Coq) ← reasoning system

Goldbach's conjecture: Every even integer > 2 is a sum of 2 primes.

↓
"Conjecture" → Truth is not known.

Program checking, chip testing, CS theory.

Mathematical proof = chain of logical deductions that leads to the proposition from a set of axioms.

Theorem: If $0 \le x \le 2$, then $-x^3+4x+1>0$.

Proof: $x \cdot x^2 \le 4x$. $\Rightarrow$ $-x^3+4x \ge 0$. $\Rightarrow$ $-x^3+4x+1>0$.

If P then Q. } "Implication"

P: $0 \le x \le 2$.

Q: $-x^3+4x+1>0$.

Is n prime?

$n \to$ variable.

Predicate: $P(n)$ ← variable.

True or false depending on value of n.

$P(4) =$ false

$P(19) =$ true.

for $i = 2$ to ... $\cancel{(n-1)}$ $\sqrt{n}$.

if i divides n.

if YES, say n is not prime

if none divide, say <u>yes</u>.

→ set of steps gives the correct answers.

Proof of correctness: If n is prime → procedure gives correct answer.

If n is not prime: then $n = xy$; $x, y \in \{2, \dots n-1\}$.

(Suppose $x > \sqrt{n}$ and $y > \sqrt{n}$) $\Rightarrow$ $x \cdot y > n$. $\Rightarrow$ n should have a factor $\leq \sqrt{n}$.

Above is a proof by <u>contradiction</u>.

<u>Axioms for us</u> : $\underline{Z} F C$ axioms.

$$\underbrace{\text{(Zeremelo-Frankel)} + \text{Axiom of choice}}$$

↓

2+2=4 would take a long series of steps

$\underbrace{\text{If } \underline{P} \text{ then } Q}$ → is another proposition.

<u>Truth Table</u>.

P	Q	$\overbrace{\text{If P then Q}}^{R}$
T	T	T
T	F	F
F	T	T
F	F	T

} True.

If $\underbrace{0 \leq x \leq 2}_{P}$ then $\underbrace{x^2 > 5}_{Q}$.

$R : (P \Rightarrow Q)$

"P implies Q"

$P \Rightarrow Q$. If P then Q.

(If P then Q).

P: it rains here today.

Q: I pay person A Rs. 100.

If it does not rain (P is False), I can either pay or not.

$P \Rightarrow Q$ is true in either case!

<u>Proof by contrapositive</u>:

If $r > 0$ is irrational, $\sqrt{r}$ is also irrational.

"not rational" "not rational"

(P1) r is not rational $\qquad\qquad$ $\sqrt{r}$ is not rational.

$$\frac{(P \Rightarrow Q)}{(\neg Q \Rightarrow \neg P)}$$

equivalent $\equiv$

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T		
F	F		
T	F		
F	T		

(P2) $\sqrt{r}$ is rational then r is rational

Suppose $\sqrt{r} = p/q$, for some $p, q \in \mathbb{Z}$.

$$r = \frac{p^2}{q^2}.$$

; since p^2, q^2 are both integers.

r is rational.

A *bogus* proof

- Show that for all non-negative integers a, b: $\frac{a+b}{2} \geq \sqrt{ab}$

$$
\begin{aligned}
\frac{a+b}{2} &\overset{?}{\geq} \sqrt{ab}, && \text{so} \\
a+b &\overset{?}{\geq} 2\sqrt{ab}, && \text{so} \\
a^2 + 2ab + b^2 &\overset{?}{\geq} 4ab, && \text{so} \\
a^2 - 2ab + b^2 &\overset{?}{\geq} 0, && \text{so} \\
(a-b)^2 &\geq 0 && \text{which we know is true.}
\end{aligned}
$$

What is a good proof?

- A proof that the number of primes is infinite by Sam Northshield

Suppose there are only finitely many primes and let P be their product. Then

$$0 < \prod_p \sin\left(\frac{\pi}{p}\right) = \prod_p \sin\left(\frac{\pi(1+2P)}{p}\right) = 0$$

What is a good proof?

- Show that $\sqrt[3]{2}$ is irrational

Next time

- Well Ordering Principle, Proof by Induction