Discrete Mathematics 31st July, 2019

Lecture 3: Proof Techniques

Instructor: Sourav Chakraborty *Scribe: Abhirup Gupta*

We can think of proof techniques like $A \implies B$ where A is a set of *assumptions* and B is the set of *deductions*.

There are 5 kinds of proofs:-

1. Constructive Proof
2. Contradiction
3. Contrapositive
4. Counter-Example
5. Induction

Constructive proof

This kind of proof is like you start with an *assumption* A and you get a *deduction* B using some reductions from A.

$$A \implies \cdots \implies B$$

. Or you may prove this in the following 2 ways:-

1.

$$A = (X \vee Y)$$
$$(A \implies B) = (X \implies B) \wedge (Y \implies B)$$

2.

$$A = (X \wedge Y)$$
$$(A \implies B) = (X \implies B) \vee (Y \implies B)$$

This kind of proof by breaking the domain into *chunks* is known as **case study proof**

You may have finite of them instead of just X and Y.
So we may use,

$$A = (X_1 \vee X_2 \vee \ldots X_k)$$
$$A \implies B \equiv \bigwedge_{i=1}^{k} (X_i \implies B)$$

Here we must remember that k is finite.

Question 1 *If p is a prime, $p > 3$ then, prove that*

$$p^2 \equiv 1(mod 6)$$

To prove: $6 \mid p^2 - 1$.
Proof. $p^2 \equiv 1(mod 2)$ [$p^2 - 1$ is even]
We need to prove $p^2 \equiv 1(mod 3)$. So there are two cases:-

$$p \equiv 1(mod 3)$$
$$p \equiv 2(mod 3)$$

If $p \equiv 1(mod 3)$ then $p = 3k + 1$ where $k \in \mathbb{Z}$ then $p^2 = 9k^2 + 6k + 1$. Since the first *two* terms are divsible by 3 the *remainder* is 1. So $p^2 \equiv 1(mod 3)$.

If $p \equiv 2(mod 3)$ then $p = 3k + 2$ where $k \in \mathbb{Z}$, then $p^2 = 9k^2 + 12k + 4$. Since the first *two* terms are diisible by 3 and 4 can be divided by 3 leaving a *remainder* of 1, $p^2 \equiv 1(mod 3)$.

So, we know,

$$p^2 \equiv 1(mod 2)$$
$$p^2 \equiv 1(mod 3)$$

So, we can say that $p^2 \equiv 1(mod 6)$. □

Proof by Contradiction

This says that

$$(A \implies B) \equiv [\neg(A \implies B) \implies F] \equiv [(A \wedge \neg B) \implies F]$$

. If you start with A and $\neg B$,then you end up getting a *false* statement.

Rational number is of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ (assuming $(a, b) = 1$) where (a, b) represents the *gcd* of a and b.

The number of steps required to acquire the gcd of two numbers is log of the larger number.

We can denote the set of **real** numbers to be a disjoint union ($\cup^+$) of the set of **rationals** , **irrational** and **transcendental** numbers.

$$\mathbb{R} = Rationals \ \cup^+ \ Irrational \ \cup^+ \ transcendental$$

Irrational numbers are those numbers which appear as the *root* of a *polynomial* e.g. $\sqrt{2}$.
Transcendental are numbers which are neither *rational* nor *irrational* e.g. e, π.

Question 2 *Prove that $\sqrt{2}$ is not rational.*

Proof. We try to prove this problem by **contradiction**.

Let's assume that $\sqrt{2}$ is *rational*. So, we can represent it in the form of $\frac{a}{b}$ where $a, b \in \mathbb{Z}^+$ and $(a, b) = 1$.

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \\ \implies a^2 &= 2b^2 \\ \implies \frac{a^2}{2} &= b^2 \qquad b^2 \in \mathbb{Z}^+ \end{aligned}$$

So, a^2 is divisible by 2.
$2 \mid a^2$, so either first a or second a is divisible by 2.
$2 \mid a \implies 4 \mid a^2$. Let $a^2 = 4k$ where $k \in \mathbb{Z}^+$. So $4k = 2b^2 \implies b^2 = 2k \implies k = \frac{b^2}{2}$.
Since, $k \in \mathbb{Z}^+$, $2 \mid b^2 \implies 2 \mid b$ and since $2 \mid a$ and $2 \mid b$ that *contradicts* our assumption since $(a, b) = 1$. □

Contrapositive

$$A \implies B \equiv (\neg B \implies \neg A)$$

Question 3 *If ab is rational then either a and b are both rational or a and b are both irrational.*

So, proving by *contrapositive* if a is rational, b is not rational and if b is rational, a is not rational.
Proof. We have two parts:-

$$a \notin \mathbb{Q}, b \in \mathbb{Q} \implies ab \notin \mathbb{Q}$$
$$a \in \mathbb{Q}, b \notin \mathbb{Q} \implies ab \notin \mathbb{Q}$$

For the first case , let us try to prove by *contradiction* i.e. $a \notin \mathbb{Q}, b \in \mathbb{Q} \implies ab \in \mathbb{Q}$ b is rational. So we can write b in the form of $\frac{b_1}{b_2}$ for some integers b_1, b_2. However a is not rational. Since ab is assumed to be rational, we can write ab as $\frac{r}{s}$ for some integers r, s. So, we can write:-

$$\begin{aligned} a &= \frac{ab}{b} \\ &= \frac{(r/s)}{b_1/b_2} \\ &= \frac{rb_2}{sb_1} \end{aligned}$$

So if $ab \in \mathbb{Q}$ a turns out to be *rational* as both rb_2 and sb_1 are integers. So, *contradiction.*

Again for the second case, we can write a as $\frac{a_1}{a_2}$ for some integers a_1, a_2.So, if we want to prove that ab is *rational* then again ab can be represented as r/s for some integers r and s. So, we can write:-

$$\begin{aligned} b &= \frac{ab}{a} \\ &= \frac{(r/s)}{a_1/a_2} \\ &= \frac{ra_2}{sa_1} \end{aligned}$$

So since b can be represented in the form of $\frac{ra_2}{sa_1}$ where ra_2 and sa_1 are both *integers*, b is a *rational* number. Our assumption for the second was that b is an *irrational* number. Hence *contradiction*.

So for ab to be *rational*, a and b should be both *rational* or both *irrational*. □

Counter Example

Many times we may need to *prove* or *disprove* a statement. If it is written like $\forall x P(x)$ where $P(x)$ is a *proposition*, then we need to give a **formal proof**.
If we want to *disprove* the above statement then we should *prove* that $\exists x \neg P(x)$. Since this statement has $\exists$ we need not prove it for all x. Just an example works. That example is called the *counter example* to $\forall x P(x)$.

Remark 1 *If prove contains an* $\exists$ *then proof can contain an example. So disprove of* $\exists$ *i.e.* $\forall$ *will need a proof.*

Induction

Induct on n where $n \in \mathbb{Z}$. We are trying to answer whether:-

$$\forall n \; A(n) \implies B(n)$$
$$\forall \, n \; P(n) \; where \; P(n) \; is \; A(n) \implies B(n)$$

These two cases have to be equivalently proved if n is *infinite*.
So an *induction* on n where $n \in \mathbb{N}$ can be broken up into the following 3 cases:-

1. **Base case** (Start point) $\implies$ This point *may* change with the induction you apply.

2. **Induction Hypothesis** : Let P_k be *true*.

3. **Inductive Step** : P_k is *true* $\implies$ P_{k+1} is *true*.

Note : *Sometimes some inductive **rules** may be required.*

Let us prove **AM - GM inequality**.

Question 4 *Prove AM - GM inequality.*

Proof. We need to show that $\forall x_1, x_2, \ldots, x_n$

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \ldots x_n}$$

First, we check for the base case $n = 1$ for which $x_1 \geq x_1$ which is *true*.
For $n = 2$,

$$\frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2}$$
$$\implies (\sqrt{x_1} - \sqrt{x_2})^2 \geq 0$$
$$\implies x_1 + x_2 \geq 2\sqrt{x_1 x_2}$$

For $n = 4$,

$$\begin{aligned}\frac{x_1 + x_2 + x_3 + x_4}{4} &= \frac{\frac{x_1+x_2}{2} + \frac{x_3+x_4}{2}}{2} \\ &\geq \frac{\sqrt{x_1 x_2} + \sqrt{x_3 x_4}}{2} \\ &\geq \sqrt{\sqrt{x_1 x_2}\sqrt{x_3 x_4}} \\ &\geq \sqrt[4]{x_1 x_2 x_3 x_4}\end{aligned}$$

So we can prove P_4 using P_2 and hence we can prove for any $k \in \mathbb{N}$ $P_k \implies P_{2k}$

Now we need to cover the *entire* real number line. So we must also prove that $P_k \implies P_{k-1}$.

$\forall x_1 \dots x_{k-1}$, We need to prove,

$$\frac{x_1 + x_2 + \ldots + x_{k-1}}{k-1} \geq \sqrt[k-1]{x_1 \dots x_{k-1}}$$

We know the **AM - GM inequality** holds for P_k, so,

$$\frac{x_1 + x_2 + \cdots + x_{k-1} + x_k}{k} \geq \sqrt[k]{x_1 \dots x_k}$$

Let us *assume* that $x_k = \frac{x_1 + \cdots + x_{k-1}}{k-1}$, then

$$\frac{x_1 + \cdots + x_{k-1}}{k-1} \geq \sqrt[k]{x1 \dots x_{k-1}(\frac{x_1 + \cdots + x_{k-1}}{k-1})}$$
$$(\frac{x_1 + \cdots + x_{k-1}}{k-1})^{\frac{k-1}{k}} \geq (x_1 \dots x_{k-1})^{\frac{1}{k}}$$

Taking both sides to a *power* of $\frac{k}{k-1}$, we get

$$\frac{x_1 + \cdots + x_{k-1}}{k-1} \geq \sqrt[k-1]{x_1 \dots x_{k-1}}$$

Hence, proving P_{k-1} and completing the proof.

Remark 2 *Say what it is we are doing and why the technique is viable for the whole real line.*

□