# Lecture 2

# Definitions, Theorems, and Proofs, Types of Proof

**Lecture-2** **PO 1 & PSO 1**

## Introduction

Unfortunately, finding proofs isn't always easy. It can't be reduced to a simple set of rules or processes. First, the statement is carefully read which is to be proved. Understand the entire notation and then rewriting the statement in our own words. It is broken down and each part is considered separately. For example to prove "$P$ if and only if $Q$", often written "$P$ iff $Q$", where both $P$ and $Q$ are mathematical statements. This notation is shorthand for a two-part statement. The first part is "$P$ only if $Q$," which means: If $P$ is true, then $Q$ is true, written $P \to Q$. The second is "$P$ if $Q$," which means: If $Q$ is true, then $P$ is true, written $Q \to P$. The first of these parts is the forward direction of the original statement and the second is the reverse direction. We write "$P$ if and only if $Q$" as $P \leftrightarrow Q$. To prove a statement of this form, you must prove each of the two directions. Often, one of these directions is easier to prove than the other. Hence, before proving anything the following points to be there in our mind.

☞ ***Definition*** means the description of an object and mathematical notations used.

☞ ***Mathematical statements*** express the attributes of an object which may or may not be true but precise.

☞ ***Proof*** is convincing logical argument that a statement is true.

☞ ***Theorem*** is a mathematical statement proved true.

☞ Some statements are proved as they assist in proving some other more significant statements are called ***lemmas***.

☞ A theorem / proof which allows to conclude that some other related statements are true, are called ***corollary***.

## 2.1 Types of Proof

Several types of arguments arise frequently in mathematical proofs. Here, we describe a few that often occur in the theory of computation. Note that a proof may contain more than one type of argument because the proof may contain within it several different sub-proofs.

### Proof by Construction

Many theorems state that a particular type of object exists. One way to prove such a theorem is by demonstrating how to construct the object. This technique is a proof by construction.

**Example 2.1** Prove that for each even number $n$ greater than 2, there exists a 3-regular graph with $n$ nodes.

Proof:

Let $n$ be an even number greater than 2.

Construct graph $G = (V, E)$ with $n$ nodes as follows.

The set of nodes of $G$ is $V = \{0, 1, ..., n-1\}$, and the set of edges of $G$ is the set

$E = \{(i, i+1) \mid \text{for } 0 \leq i \leq n-2\} \cup \{(n-1, 0)\} \cup \{(i, i+n/2) \mid \text{for } 0 \leq i \leq n/2-1\}$.

Picture the nodes of this graph written consecutively around the circumference of a circle. In that case, the edges described in the top line of $E$ go between adjacent pairs around the circle. The edges described in the bottom line of $E$ go between nodes on opposite sides of the circle.

This mental picture clearly shows that every node in $G$ has degree 3.

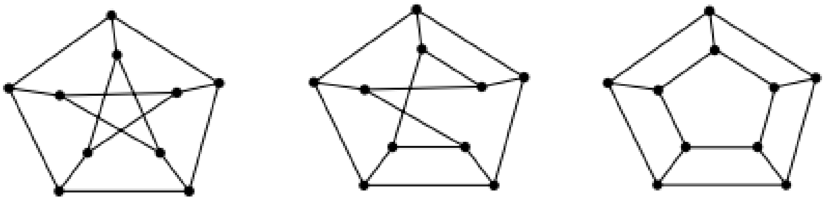

Figure 2.1: Representation of 3 regular graph.

The above figures show that every node in the graph $G$ has degree 3 and the graph is 3 regular.

### Proof by Contradiction

In one common form of argument for proving a theorem, we assume that the theorem is false and then show that this assumption leads to an obviously false consequence, called a contradiction. We use this type of reasoning frequently in everyday life, as in the following example.

**Example 2.2** Prove that $\sqrt{2}$ is an irrational number.

Proof:
First, we assume for the purpose of later obtaining a contradiction that $\sqrt{2}$ is rational.
Thus $\sqrt{2} = m/n$,
where $m$ and $n$ are integers. If both $m$ and $n$ are divisible by the same integer greater than 1, divide both by the largest such integer. Doing so doesn't change the value of the fraction. Now, at least one of $m$ and $n$ must be an odd number.
We multiply both sides of the equation by $n$ and obtain

$$\sqrt{2}n = m$$

We square both sides and obtain

$$2n^2 = m^2$$

Because $m^2$ is 2 times the integer $n^2$, we know that $m^2$ is even.
Therefore, $m$, too, is even, as the square of an odd number always is odd.
So we can write $m = 2k$ for some integer $k$.
Then, substituting $2k$ for $m$, we get

$$2n^2 = (2k)^2 = 4k^2$$

Dividing both sides by 2, we obtain

$$n^2 = 2k^2$$

But this result shows that $n^2$ is even and hence that $n$ is even
Thus we have established that both $m$ and $n$ are even.
But we had earlier reduced $m$ and $n$ so that they were not both even—a contradiction.
Hence, $\sqrt{2}$ is an irrational number.

## Proof by Induction

Proof by induction is an advanced method used to show that all elements of an infinite set have a specified property. For example, we may use a proof by induction to show that an arithmetic expression computes a desired quantity for every assignment to its variables, or that a program works correctly at all steps or for all inputs.
The format for writing down a proof by induction is as follows given in an example:
**Example 2.3** Prove that $P_t = PM^t - Y((M^t - 1)/(M - 1))$ for all $t \geq 0$ .
Proof:
Basis: Prove that the formula is true for $t = 0$ . If $t = 0$, then the formula states that

$$P_0 = PM^0 - Y((M^0 - 1)/(M - 1)) \ .$$

We can simplify the right-hand side by observing that $M^0 = 1$. Thus we get $P_0 = P$ which holds because we have defined $P_0$ to be $P$ . Therefore, we have proved that the basis of the induction is true.
Induction Step: For each $k \geq 0$ , assume that the formula is true for $t = k$ and show that it is true for $t = k + 1$ .
The induction hypothesis states that

$$P_k = PM^k - Y((M^k - 1)/(M - 1))$$

Our objective is to prove that

$$P_{(k+1)} = PM^{(k+1)} - Y((M^{(k+1)} - 1)/(M - 1))$$

We do so with the following steps.
First, from the definition of $P_{(k+1)}$ from $P_k$ , we know that $P_{(k+1)} = P_k M - Y$.
Therefore, using the induction hypothesis to calculate P$_k$

$$\mathrm{P}_{(k+1)} = [PM^k - Y((M^k - 1)/(M - 1))]M - Y$$

Multiplying through by $M$ and rewriting $Y$ yields

$$\begin{aligned} P_{(k+1)} &= PM^{(k+1)} - Y((M^{(k+1)} - M)/(M - 1)) - Y((M - 1)/(M - 1)) \\ &= PM^{(k+1)} - Y((M^{(k+1)} - 1)/(M - 1)) \ . \end{aligned}$$

Thus the formula is correct for $t = k + 1$ , which proves the theorem.

**Example 2.4** Prove that $1 + x + x^2 + x^3 + \cdots\ldots\ldots\ldots\ldots + x^n = (1 - x^{n+1})/(1 - x)$ for all $n \geq 0$.
Proof:
Basis: We need to prove that the given statement is true for $n = 0$. If $n = 0$ the LHS of the formula becomes 1 and RHS becomes $(1 - x^1)/(1 - x) = 1$. Hence basis is proved.
Induction Step: Let the given statement is true for $n = k$.
Therefore we can write

$$P_k \equiv 1 + x + x^2 + x^3 + \cdots\ldots\ldots\ldots\ldots + x^k = (1 - x^{k+1})/(1 - x).$$

Now we have to prove for $n = k + 1$ i.e.

$$P_(k + 1) \equiv 1 + x + x^2 + x^3 + \cdots\ldots\ldots\ldots\ldots + x^k + x^{k+1} = (1 - x^{k+2})/(1 - x) \ .$$

$$\begin{aligned} \text{LHS for } P_(k + 1) &= 1 + x + x^2 + x^3 + \cdots\ldots\ldots\ldots\ldots + x^k + x^{k+1} \\ &= (1 - x^{k+1})/(1 - x) + x^{k+1} \\ &= (1 - x^{k+2})/(1 - x) \\ &= RHS. \end{aligned}$$

Hence $P_n$ is true for all $n \geq 0$.