Lecture 2: Proofs

Nitin Saxena*

IIT Kanpur

All of you must have proved a lot of mathematical statements by now and have pretty good intuition about what proofs are. So we will take an informal approach of proofs. The ideas of rigorous and correct mathematical proofs will be shown through examples. A more formal approach can be taken through logic, a brief introduction to logic is given at the end of these course notes and is meant as an advanced reading.

Exercise 1. Recall the formula for the infinite geometric sum. Using that, one can deduce the following:

$$\begin{aligned}
&\cdots + x^{-2} + x^{-1} + 1 + x + x^2 + \cdots \\
&= \frac{x^{-1}}{1 - x^{-1}} + \frac{1}{1 - x} \\
&= \frac{1}{x - 1} + \frac{1}{1 - x} \\
&= 0\,.
\end{aligned}$$

What could be the problem?

One of the applications of the formula is incorrect!

1 What is a Proof?

A *proof* of a statement is a correct mathematical argument which ultimately shows that the statement is true. A proof, in general, consists of a series of mathematical steps, where any step is derived (implied) from the previous step or is part of the axioms, definitions, hypotheses or premises. *Hypothesis* (or *premise*) is the mathematical statement given to us.

Axioms are the things we assume to be true in a mathematical system.

Example 1 (Euclid's axioms). – There is a unique line from any point to any point.
– There is a unique circle with any center and radius.

Suppose we want to prove, "If n is odd, then n^2 is odd".

Proof. n is odd (hypothesis)
$\Leftrightarrow$ $n = 2k + 1$ (definition of odd)
$\Leftrightarrow$ $n^2 = 4k^2 + 4k + 1$
$\Leftrightarrow$ $n^2 = 2(2k^2 + 2k) + 1$
$\Rightarrow$ n^2 is odd (definition of odd) □

Exercise 2. Why do we have one-directional arrow in a step and bidirectional ones in the others?

To assert that some statements may not be equivalent.

The implications from one step to another is the critical part and most of the mistakes happen there. We need to make sure that every implication either follows from an hypothesis/axiom/definition or are "straightforward" enough.

The *conclusion* part of an implication is usually asserted by the words: hence, thus, therefore, consequently, whence, etc.

* Edited from Rajat Mittal's notes.

Most of the theorems can be seen as one mathematical statement implying another. Let us represent the mathematical statements as p, q. Then we will write $p \Rightarrow q$ for the fact that statement p implies statement q. Another important concept is *equivalence*, $p \Leftrightarrow q$, which is the same as saying that $p \Rightarrow q$ and $q \Rightarrow p$. The latter is called the *converse* of the former, and vice-versa.

For example, in the statement "If n is odd, then n^2 is odd", we can represent "n is odd" as p and "n^2 is odd" as q. Then the statement is $p \Rightarrow q$.

The English statements of "if-then" are implications and "iff/if and only if" are equivalences. Consider the following theorems.

- If n is odd then n^2 is of the form $4k + 1$.
- For all primes, a^p leaves a remainder a when divided by p.
- Every prime greater than 2 is odd.
- $\sqrt{2}$ is irrational.
- n^2 is even if n is even.

Exercise 3. Represent each of these theorems in the form $p \Rightarrow q$ or $p \Leftrightarrow q$.

Now we will look at various techniques by which theorems can be proved. These include direct proofs, contrapositive, proof by contradiction and proof by induction.

2 Direct proofs

This is the most obvious way of proving truth. If we need to prove $p \Rightarrow q$, we start with p, derive different mathematical statements which end at q. The initial example given above for showing that n^2 is odd if n is odd was proven using direct proof.

Let us take another example. Suppose we want to show: All perfect squares are of the form $4k$ or $4k + 1$.

Proof. n is either even or odd.
$\Rightarrow$ n is of the form $2k$ or $2k + 1$.
$\Rightarrow$ Squaring, $n^2 = 4k^2$ or $n^2 = 4k^2 + 4k + 1$.
$\Rightarrow$ Hence, n^2 is of the form $4k$ or $4k + 1$. □

This is an "indirect" proof of: $4k + 2, 4k + 3$ are never perfect squares!

2.1 Quantification

Many a times the theorems given in mathematics require quantification over a large domain. That means the statements look like,

1. Existential: *There exist* an element of the universe (i.e. a mathematical object) which satisfies certain condition.
2. Universal: *For all* elements of the universe certain condition is satisfied.

Note 1. Mathematical universe is the set of elements we are interested in. For example, natural numbers $\mathbb{N}$, integers $\mathbb{Z}$, rationals $\mathbb{Q}$, reals $\mathbb{R}$ or complex numbers $\mathbb{C}$.

A direct proof of an existential kind of a theorem can be given by an *example*.

Prove that there is a prime of the form $4k + 1$.

Proof. Consider the number 5. It is of the form $4k + 1$ and we know that 5 is a prime. Hence, there is a prime of the form $4k + 1$. □

Similarly, a direct refutation of a universal kind of a theorem can be given by a *counterexample*. Prove that all primes are of the form $4k + 1$.

Proof. Consider the number 3. It is not of the form $4k + 1$ and we know that 3 is a prime. Hence all primes need not be of the form $4k + 1$. □

It is convenient to use the notation $\exists x \in U$ (resp. $\forall x \in U$) to mean "there exists an element x in the universe U" ("for all elements x in the universe U").

Exercise 4. What is the relation between proving an existential kind of theorem and refuting a universal kind of theorem?

Negation of an existential statement is a universal one.

References

1. K. H. Rosen. Discrete Mathematics and Its Applications. *McGraw-Hill*, 1999.