Lecture 3: Proofs

Nitin Saxena[⋆]

IIT Kanpur

1 Contrapositive proofs

A slightly more involved way of proving $p \Rightarrow q$ is to prove that if q is false then p is false too. Denote *not* (negation) of a statement p by $\neg p$. A proof by contrapositivity involves showing $\neg q \Rightarrow \neg p$ instead of showing $p \Rightarrow q$.

What does this mean in natural language. Consider the statement, if Raman goes to market then Marie will not go to the market. Clearly, if Marie is in the market then it means that Raman did not go the market.

Let us look at some mathematical examples. Show that if there is a prime $n > 3$ then $n + 1$ is not a perfect square. Here p is "$n \geq 3$ is a prime number" and q is "$n + 1$ is not a perfect square".

Proof. We will start with $\neg q$, i.e., $n + 1$ is a perfect square.
$\Rightarrow$ there exist x, s.t., $x^2 = n + 1$.
$\Rightarrow x^2 - 1 = n$.
$\Rightarrow n$ can be factored as $(x + 1)(x - 1)$, where $(x - 1) \neq 1$.
$\Rightarrow n$ is not a prime. □

Note 1. The previous theorem can be equivalently stated as, there is no prime number $n > 3$ for which $n+1$ is a perfect square.

Exercise 1. Convince yourself that direct proof of the previous theorem will be difficult.

Warning: There is a common fallacy, where instead of proving $\neg q \Rightarrow \neg p$ some people prove $\neg p \Rightarrow \neg q$. You should be very careful, $\neg p \Rightarrow \neg q$ is NOT equivalent to $p \Rightarrow q$.

Example 1. Consider the statement: If n is not of the form $6k + 3$ then n^2 is not divisible by 3. You can check that this statement is not true. On the other hand, we can prove $\neg p \Rightarrow \neg q$ in this case.

$\neg p$ means that n is of the form $6k + 3$. On squaring, $n^2 = 36k^2 + 36k + 9 = 3(12k^2 + 12k + 3)$. So, $\neg q$ is true (3 divides n^2).

2 Contradiction

Another technique, related to contrapositivity, is the method of contradiction. In this case, if we want to prove that p is true, then we assume $\neg p$ and arrive at something false (like 2 is an odd number, etc.) or something contrary to the hypothesis.

The first example of a proof by contradiction will be the fact that $\sqrt{2}$ is not rational.

Proof. Suppose $\sqrt{2}$ is rational. This implies that there exist $a, b \in \mathbb{N}$ with no common factor s.t. $\sqrt{2} = \frac{a}{b}$. Squaring, $2 = \frac{a^2}{b^2}$. This implies that there is a common factor (namely, 2) between a and b. But this violates the hypothesis that a and b have no factor in common. This is a contradiction. □

Exercise 2. Prove that if $2 = \frac{a^2}{b^2}$ then a and b have 2 as a common factor.

From $a^2 = 2b^2$ one can deduce that 2 divides a. Say, $a = 2a'$.
Then we get $2a'^2 = b^2$, which implies that 2 divides b.

[⋆] Edited from Rajat Mittal's notes.

Let us consider another theorem.

Theorem 1 (Euclid, c. 300 BC). *Given a natural number n, there exist a prime greater than n.*

Proof. Suppose there is no prime greater than n. Define $m = n! + 1$. Since $m - 1$ is divisible by all the numbers $\{2, \cdots, n\}$, m is not divisible by any of them. This implies that no prime divides m (because all primes are smaller than n). Thus, m itself has to be a prime greater than n. This is a contradiction. □

Our last example will require some definitions in set theory. It is easy to define *cardinality* of a set (size of a set) when the set is finite. It is the number of elements in the set. How about the "cardinality" when the set is infinite. Would you say that the cardinality of the set of odd integers O is the same as the cardinality of the set of even integers E?

The intuition seems to suggest that they should be the same ($|O| = |E|$?). The reason being that you can establish a one to one relation between the two sets, e.g. $x \rightarrow x - 1$, which covers entire sets.

Note 2. We denote the cardinality of a set S by $|S|$.

The *cardinality* for any two sets are defined to be equal if there is a bijection between the two sets. Remember that *bijection* means the relation is one to one and onto.

Similarly, we can say that $|S| \leq |T|$ if there is an injection (one to one mapping) from S to T. There is a theorem (Schröder-Bernstein) which states that if there are injections from S to T and T to S then there is a bijection between S and T.

You will prove in the assignment that the cardinality of natural numbers is same as cardinality of integers. The same can be shown for integers and rationals. Though, the number of rationals and number of reals are not the same. Things can get weird at infinity !!

Let us see another beautiful proof by contradiction.

Theorem 2. *The cardinality of a set S is not equal to the cardinality of its powerset 2^S (set of all subsets).*

Note 3. This statement sounds trivial if the set is finite. But we will prove this even for infinite sets.

References

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