Lecture 2: Proofs

Rajat Mittal

IIT Kanpur

All of you must have proved 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.

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 axioms, definitions or hypothesis. The axioms are the things we assume to be true. Hypothesis is the mathematical statement given to us.

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

Exercise 1. Why do we have one directional arrows in few steps and bidirectional in others?

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 hypothesis/axioms/definitions or are straightforward enough.

Most of the theorems can be seen as one mathematical statement implying another. Lets 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 same as saying that $p \Rightarrow q$ and $q \Rightarrow p$. 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.
- All primes are odd.
- $\sqrt{2}$ is irrational.
- n^2 is even if n is even.

Exercise 2. 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 direct way of showing a theorem. 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.

Lets take another example. Suppose we want to show, all perfect squares are of the form $4k$ or $4k+1$.

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

2.1 Quantification

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

1. Existential: *There exist* an element of the universe (mathematical not physical) 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, reals or complex numbers.

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 7. It is not of the form $4k+1$ and we know that 7 is a prime. Hence all primes need not be of the form $4k+1$. □

Exercise 3. What is the relation between proving an existential kind of theorem and refuting a universal kind of theorem.

3 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, implies, Raman did not go the market.

Lets look at some of the mathematical examples. Show that if there is prime number $n > 3$ 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 $(x+1)(x-1)$.
$\Rightarrow$ n is not a prime. □

Note 2. The previous theorem can be equivalently stated as, there is no prime number $n > 3$ for which $n+1$ is a perfect square.

Exercise 4. Convince yourself that direct proof of the previous theorem will be difficult.

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 $p \Rightarrow q$. Rather $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$.

Consider the statement that if n is composite or not of the from $6k+3$ then n^2 is not divisible by 3. You can check that this statement is not true. Though we can prove $\neg p \Rightarrow \neg q$ in this case.

$\neg p$ will be that n is prime and of the form $6k+3$. If we square, $n^2 = 36k^2 + 36k + 9 = 3(12k^2 + 12k + 3)$. So $\neg q$ is true (3 divides n^2).

4 Contradiction

Another related technique with 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 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 between a and b. But this violates the hypothesis that a and b have no factor in common. This is a contradiction. □

Exercise 5. Prove that if $2 = \frac{a^2}{b^2}$ then a and b have a common factor of 2.

Lets consider another theorem.

Theorem 1. *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).

By fundamental theorem of arithmetic any number can be factorized into product of primes. But m does not have any prime factor. 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 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 relationship between the two sets, e.g., $x \to x - 1$, which covers entire sets.

Note 3. 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, Schroder-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. It can also be shown that the number of integers is equal to the number of rational numbers. Though the number of rational and number of reals are not the same. Things can get weird at infinity !!

Lets 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 4. This statement sounds trivial if the set is finite. But we will prove this even for infinite sets.

Proof. Suppose the cardinality of the set and its superset are equal. By definition, there exists a bijection between the set and its superset. Let $\phi : S \to 2^S$ be the bijection. Define a new subset of S,

$$T = \{x : \ x \in S, \ x \notin \phi(x)\}$$

In words, T is the set of elements of S which are not in their image (under ϕ).

By definition T is an element of 2^S. Since ϕ is a bijection, T will have a pre-image $t \in S$. Consider the two cases,

Case 1: Suppose $t \in T$. Since t is in its image, it should not be in the special set T (by definition). So $t \notin T$, a contradiction.

Case 2: Suppose $t \notin T$. Since t is not in its image, it should be in the special set T. So $t \in T$, again a contradiction.

Since two cases cover all possibilities, we proved that bijection can't exist. Hence the cardinality of S and 2^S are different.

Another way to look at the same proof is the following. Look at the diagonal matrix below. Here x_i's in the first row are elements of the set S. X_i in the first column represents $\phi(x_i)$. The i, j entry of the $0-1$ matrix denotes if x_j is an element of X_i.

	x_1	x_2	x_3	$\cdots$
X_1	0	1	0	$\cdots$
X_2	1	0	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Look at the diagonal elements of the $0-1$ matrix and flip them. The subset corresponding to them (T in the previous proof) is not mapped to any element of S. Because it is different from every subset at at least one position (the diagonal one). □

The second argument of the proof is known as diagonalization argument. It is used to prove that integers and reals cannot have a bijection. The sets which have cardinality less than or equal to integers/natural numbers/rational are known as *countable sets* and the sets having cardinality greater than integers (like reals) are called *uncountable sets*.

5 Induction

Mathematical induction is one of the strongest tools to prove universal statements about natural numbers (statements like "for all natural numbers n, $n \leq 2^n$"). For the use of induction, the range of the universal statement should be countable.

Say we want to prove $\forall x : P(x)$ where $x \in \mathbb{N}$ and $P(x)$ is a property of x. Then mathematical induction proceeds by showing two things.

1. Base: $P(0)$ is true.
2. Induction: If $P(m)$ is true then $P(m+1)$ is true. "$P(m)$ is true" is known as induction hypothesis.

This seemingly simple technique has lot of variations and can prove very complicated theorems. Let us start with a simple example.

Theorem 3. *Prove that* $0 + 1 + 4 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof. Let $P(n)$ be the hypothesis that $0 + 1 + 4 + 9 + \cdots + n^2 = n(n+1)(2n+1)/6$.

Base: $P(0)$ means that $0 = \frac{0 \times 1 \times 1}{6}$.

Induction: For the inductive step we need to show,

$$0 + 1 + \cdots + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

By induction hypothesis, $0 + 1 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$. Adding $(n+1)^2$ to both the sides,

$$0 + 1 + \cdots + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2.$$

Exercise 6. Show that $\frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$.

Hence we complete the induction and prove the theorem.

□

Let us try another example.

Theorem 4. *Show that every number $n > 0$ can be written in a binary representation.*

$$n = b_r 2^r + \cdots + 2b_1 + b_0$$

Where r is some integer and $b_0, b_1, \cdots, b_r$ are bits (0/1).

Proof. Suppose $P(n)$ be the hypothesis that n can be written in a binary representation.

Base: $P(1)$, clearly $b_0 = 1$ gives the binary representation.

Exercise 7. Does it matter that the base case is $P(1)$ instead of $P(0)$?

Induction: We will assume a slightly different hypothesis, "$P(k)$ is true for all $k < m$", and show that $P(m)$ is true. It is easy to convince yourself that even this induction hypothesis will prove the result. But you can formally convert this into original version.

Exercise 8. Show that this new version of induction is same as old version.

Now, to prove $P(m)$. Consider two cases:

Case 1: If m is even, then $m' = \frac{m}{2}$ is an integer and is less than m. Hence m' has a binary representation.

$$m' = b_r 2^r + \cdots + 2b_1 + b_0$$

Then m will have the binary representation,

$$m = 2m' = b_r 2^{r+1} + \cdots + 2b_0 + 0 = c_{r+1} 2^{r+1} + \cdots + 2c_1 + c_0$$

Case 2: If m is odd, then $m' = \frac{m-1}{2}$ is an integer and is less than m. Hence m' has a binary representation.

$$m' = b_r 2^r + \cdots + 2b_1 + b_0$$

Then m will have the binary representation,

$$m = 2m' + 1 = b_r 2^{r+1} + \cdots + 2b_0 + 1 = c_{r+1} 2^{r+1} + \cdots + 2c_1 + c_0$$

Since these two cases exhaust all the possibilities, we are done. □

Theorem 5. *How can you prove that binary representation is unique?*

The induction technique can be modified in various ways. We will take an example of multi-dimensional induction, you can convince yourself that in spirit, this is the same as the original version.

Theorem 6. *Suppose there is a function $f(m,n)$ satisfying following equalities,*

$$f(m+1,n) = f(m,n) + 2(m+n) + 1 \text{ and } f(m,n+1) = f(m,n) + 2(m+n) + 1.$$

If $f(0,0) = 0$, show that $f(m,n) = (m+n)^2$ satisfies these constraints.

Proof. The hypothesis $P(m,n)$ represents the fact that $f(m,n) = (m+n)^2$.

Base: $f(0,0) = (0+0)^2 = 0$ is true.

Induction: We need to be careful here and need to show two steps.

1. $P(m,n)$ is true implies $P(m+1,n)$.

$$f(m+1,n) = f(m,n) + 2(m+n) + 1 = (m+n)^2 + 2(m+n) + 1 = (m+n+1)^2 = ((m+1)+n)^2$$

2. $P(m,n)$ is true implies $P(m,n+1)$.

$$f(m,n+1) = f(m,n) + 2(m+n) + 1 = (m+n)^2 + 2(m+n) + 1 = (m+(n+1))^2$$

□

We have given an informal introduction to proofs using examples. People who are interested in more formal notions of proof, should read the section below and references mentioned there. There is a separate course on logic where you will study this in much more detail.

6 Logic (Advanced)

We will call mathematical statements as propositions. For example, "n is odd" is a proposition and so is "n^2 is odd". Other examples are,

- $x + y = 3$
- $n + 1$ is prime
- $y^2 = z$
- $\frac{1}{2}$ is irrational

These propositions can be combined or operated upon by operators like AND ($\wedge$), OR ($\vee$) and NOT ($\neg$). Suppose p and q are two propositions, the operators can be specified by the truth tables. We use T to denote that proposition is true and F for false.

NOT: ¬ p

p	$\neg p$
T	F
F	T

AND: $p \wedge q$

p	q	$p \wedge q$
T	T	T
F	T	F
T	F	F
F	F	F

OR: $p \vee q$

p	q	$p \wedge q$
T	T	T
F	T	T
T	F	T
F	F	F

This operators are used in common language also and have similar meaning. The important distinction to remember is that "OR" is true if both the propositions are true too.

Another operator of importance in this context is implication, which can be defined in terms of previous operators.

Implication: $p \Rightarrow q = \neg p \vee q$

p	q	$p \Rightarrow q$
T	T	T
F	T	T
T	F	F
F	F	T

For the implication $p \Rightarrow q$, p is called the hypothesis and q is called the conclusion. So an implication is *only* false if hypothesis is T but conclusion is F. For example, the statement "n is odd and $n = 2$ implies $n^2 = 6$" is in fact true.

Exercise 9. What are the propositions and operators in the above statement?

The equivalence $p \Leftrightarrow q$ means $p \Rightarrow q$ and $q \Rightarrow p$.

Exercise 10. Make the truth table of $\Leftrightarrow$.

6.1 Quantified statements

Many theorems in mathematics involve quantification. To make sense of quantification, we need to introduce predicate's. A *predicate* is can be thought of as a function which outputs a proposition. For example, $P(x) = x \geq 3$ is a predicate which depends upon x, i.e., the truth value depends upon x. A predicate can be a function of multiple variables. So "n is odd" can also be considered a predicate with n as a variable.

There are two kinds of *quantifiers* which can be applied on a predicate.

- *Existential quantification ($\exists x : P(x)$)*: Says that there exists an element x in the *universe* which makes the predicate $P(x)$ true.
- *Universal quantification ($\forall x : P(x)$)*: Says that $P(x)$ is true for all the possible values of x in the *universe*.

The *universe* is generally clear from the context. Otherwise it is specifically stated. Lets look at some more examples.

1. There exist a natural number smaller than 0.
2. All natural numbers are real numbers.
3. Every x is equal to zero.
4. There is a y which is the square root of x.
5. For all natural x there exists a y, s.t., $y > x$.

Exercise 11. Find out the quantifiers, predicate and universe in the examples given above.

6.2 Rules of inference

The mathematical steps or statements in the proof are propositions (quantified predicates) or combination of propositions (quantified predicates). To prove a mathematical statement means to show that the value of the corresponding proposition (quantified predicate) is T (true). Many a times the statement/ theorem which needs to be proven will look like $p \Rightarrow q$.

Exercise 12. For the statement "If n is odd, then n^2 is odd", what are the propositions and what are the operators. Can you write it as an implication in terms of quantified predicate.

For a proof, we go from one step to another using *rules of inference*. Below you will find some examples of rules of inference.

- $p \vee q$ can be inferred from p.
- q can be inferred from p and $p \Rightarrow q$.
- $\neg p$ can be inferred from $\neg q$ and $p \Rightarrow q$.
- $p \Rightarrow r$ can be inferred from $p \Rightarrow q$ and $q \Rightarrow p$.
- $\exists x : P(x)$ can be inferred from $P(c)$ where c belongs to the universe.
- $P(c)$ for some element c in universe can be inferred from $\exists x : P(x)$.
- $\forall x : P(x)$ can be inferred from the fact that $P(c)$ is true for arbitrary c in universe.
- $P(c)$ for c in universe can be inferred from $\forall x : P(x)$.

Hence, a proof is a series of mathematical steps where one step can be derived from the previous one using rules of inference. For more details about logic and formal notions of proof, please read the first and third chapter of Rosen's book [1].

7 Assignment

Exercise 13. What is the relation between contrapositivity and contradiction?

Exercise 14. Show that the cardinality of integers is same as cardinality of natural numbers.

Exercise 15. Show that there is no bijection between integers and real numbers.

Hint: The proof will require diagonalization.

Exercise 16. Read the concepts of countability and uncountability.

Exercise 17. Let $f_n = f_{n-1} + f_{n-2}$ and $f_1 = f_2 = 1$. This numbers are called Fibonacci numbers. Show that $f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$.

Exercise 18. Show that a chess-board with two diagonal corners removed can't be covered (no overlaps allowed) by 2×1 tiles.

References

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