Lecture 4: Proofs

Nitin Saxena[⋆]

IIT Kanpur

Let us see another beautiful proof by contradiction.

Theorem 1. *The cardinality of a set S is not equal to the cardinality of its powerset 2^S (set of all subsets).*

Note 1. 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 powerset are equal. By definition, there exists a bijection between the set and its powerset. Let $\phi : S \to 2^S$ be a 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 the two cases cover all possibilities, we proved that a bijection cannot exist. Hence, the cardinality of S and 2^S are different.

Note 2. There is an injection from S to 2^S, but not vice-versa!

Another way to look at the same proof is the following. Look at the schematic 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)-th entry of the 0/1 matrix denotes whether x_j is an element of X_i.

$$\begin{array}{r|c|c|c|c}
 & x_1 & x_2 & x_3 & \cdots \\
\hline
\phi(x_1) = X_1 & 0 & 1 & 0 & \cdots \\
\hline
\phi(x_2) = X_2 & 1 & 0 & 0 & \cdots \\
\hline
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Look at the diagonal elements of the 0/1 matrix and flip them. The subset corresponding to the diagonal string (T in the previous proof) is not mapped to any element of 2^S. Because it is different from every subset in at least one position (namely, the diagonal one). □

This interpretation of the proof is known as the *diagonalization argument.* It is used to prove that integers and reals cannot have a bijection (Cantor 1891). The sets which have cardinality less than or equal to integers/ natural numbers /rationals are known as *countable sets.* The sets having cardinality greater than integers (like reals) are called *uncountable sets.*

1 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.

[⋆] Edited from Rajat Mittal's notes.

Note 3. Induction can be generalized to uncountables with some effort. Then, it is called *transfinite induction.* We will not go into its details.

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 case:* $P(0)$ is true.
2. *Induction step:* If $P(m)$ is true then $P(m+1)$ is true.
   "$P(m)$ is true" is called the *induction hypothesis.*

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

Theorem 2. *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,

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

Hence we complete the induction and prove the theorem.

□

Let us try another example.

Theorem 3. *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. Let $P(n)$ be the hypothesis that n can be written in a binary representation.

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

Exercise 1. 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.

Exercise 2. Show that this version of induction step reduces to the old one.

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. □

Exercise 3. How can you prove that binary representation is unique?

Use the fact that $2^n > 2^{n-1} + 2^{n-2} + \cdots + 2 + 1$.

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 4. *Suppose there is a function $f(m,n)$ satisfying the 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 "move one step in each direction".

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. Students 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 these in much more detail.

2 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	$p \vee q$
T	T	T
F	T	T
T	F	T
F	F	F

Such operators are also used in common language and they have similar meaning. The important distinction to remember is that "OR" is true if both the propositions are true (i.e. it is not *exclusive*).

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

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

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 4. What are the propositions and operators in the above statement?

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

Exercise 5. Make the truth table of $\Leftrightarrow$.

2.1 Quantified statements

Many theorems in mathematics involve quantification. To make sense of quantification, we need to introduce predicates. A *predicate* 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. Eg. "n is odd" can be considered as 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. Let us 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 6. Find out the quantifiers, predicate and universe in the examples given above.

2.2 Rules of inference

The mathematical steps or statements in a 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 7. 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 $q \Rightarrow r$.
- $\exists x : P(x)$ 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].

References

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