CSC-257
Theory Of Computation
(BSc CSIT, TU)

Ganesh Khatri
kh6ganesh@gmail.com

Methods of Proof

- **Theorem**
  - A theorem is a mathematical proposition that is true.
  - Many theorems are conditional propositions.
  - For example, if f(x) and g(x) are continuous then f(x) + g(x) are also continuous.
  - If theorem is of the form "if p then q", the p is called hypothesis and q is called conclusion
- **Proofs**
  - Trivial proof
  - Vacuous proof
  - Direct proof
  - Indirect proof
  - Proof by contradiction
  - Proof by cases
  - Proof by mathematical induction
  - Proof by counter examples

Trivial Proof

- We say is trivially true if q is true, and this kind of proof (i.e. showing q is true for without referring to p) is called a trivial proof.
- Consider an implication: $p \rightarrow q$
- If it can be shown that q is true, then the implication is always true by definition of an implication

Vacuous Proof

- Consider an implication: $p \rightarrow q$
- If it can be shown that p is false, then the implication is always true by definition of an implication.
- Note that you are showing that the antecedent is false

Direct Proof

- To prove $p \rightarrow q$ is true,
- we start assuming hypothesis p is true and we use information already available to prove q is true, and if q is true then the argument is valid. This is called direct proof
- *E.g. If a and b are odd integers, then a+b is an even integer.*
- Here a and b are odd integers. Since every odd numbers can be written by 2m+1 where m is any integer.
- So, a = 2m+1
- b = 2n+1 for some integers m and n
- Now, a+b = 2m+1+2n+1 = 2m+2n+2 = 2(m+n+1) = 2k where k = m+n+1 is any integer.
- This shows a+b is even. Proved.

Indirect proof (proof by contraposition)

- Since, $p \rightarrow q$ is equivalent to $\neg q \rightarrow \neg p$.
- To prove $p \rightarrow q$ is true, we assume the conclusion is false;
- using the fact if p becomes false, original implication is true.
- e.g. *if the product of two integers a and b is even, then either a is even or b is even*.
- Suppose, if possible both a and b are odd integers. So, $a = 2m+1$ and $b = 2n+1$.
- And $axb = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1 = 2k+1$
- where $k = 2mn+m+n$, which is not true.
- So, our original implication is true.

Proof by Contradiction

- This proof proceeds by contradiction
- That is, we will assume that the claim we are trying to prove is wrong and reach a contradiction.
- If all the derivations along the way are correct, then the only thing that can be wrong is the assumption, which was that the claim we are trying to prove does not hold.
- This proves that the claim does hold.
- *Eg: For any integer n, if n2 is odd, then n is odd*
- Suppose not. [We take the negation of the given statement and suppose it to be true.] Assume, to the contrary, that for an integer n such that n2 is odd and n is even. [We must deduce the contradiction.]

Proof by Contradiction

- By definition of even, we have, n = 2k for some integer k.
- So, by substitution we have, n . n = (2k) . (2k) = 2(2.k.k)
- Now (2.k.k) is an integer because products of integers are integer; and 2 and k are integers.
- Hence, n . n = 2 . (some integer)
- or n2 = 2 . (some integer) which is even.
- and so by definition of n2 even, is even.
- So the conclusion is since n is even, n2, which is the product of n with itself, is also even.
- This contradicts the supposition that n2 is odd. [Hence, the supposition is false and the proposition is true.]

Proof by Cases

- You can sometimes prove a statement by:
  - Dividing the situation into cases which exhaust all the possibilities; and
  - Showing that the statement follows in all cases.
- It's important to cover all the possibilities. And don't confuse this with trying examples; an example is not a proof
- Proof by cases is closely related to the idea of using If-statements in a computer program

Proof by Cases

- **Theorem.** For every integer n, $n^2 \geq n$.
- **Proof.**. By cases. There are three cases: $n \leq -1$, $n = 0$ and $n \geq 1$.
- **Case 1 : ($n == 0$).** Notice that $0^2 \geq 0$, so the theorem holds when $n = 0$
- **Case 2. ($n \geq 1$).**
  - (1) n ≥ 1 (from the condition for this case)
  - (2) n^2 ≥ n (multiply both sides of (1) by the positive value n)
  - So the theorem holds in this case
- **Case 3. ($n \leq -1$).** Since $n \leq -1$ and $n^2 \geq 0$, the theorem clearly holds in this case.

Proof by Mathematical Induction

- Mathematical induction is a powerful, yet straightforward method of proving statements whose "domain" is a subset of the set of integers
- Usually, a statement that is proven by induction is based on the set of natural numbers
- This statement can often be thought of as a function of a number n, where n = 1,2,3...
- This involves three main steps:
  - proving the base of induction,
  - forming the induction hypothesis, and
  - finally proving that the induction hypothesis holds true for all numbers in the domain

Proof by Mathematical Induction

- Theorem. For every positive integer n, $1 + 2 + ... + n = n(n+1)/2$.
- Proof. The proof is by induction.
  - Initial Step : proves the equation for $n = 1$,
  - Inductive Step : assumes the hypothesis that the equation is true for $n = k$ and proves that equation is true for $n = k+1$ so that it is true for all the cases.
- Initial Step : $n = 1$. Substituting $n = 1$ into the equation, $1 = (1)(1+1)/2$, which is clearly true.
- Inductive Step : suppose $n = k$, $k > 1$. Now if we can prove that equation is true for $n = k+1$ then we are done.
  - Goal of this step is to prove $1 + 2 + ... + k + (k+1) = (k+1)(k+2)/2$
  - Since $1 + 2 + ... + k = k(k+1)/2$ (since equation is true for $n = k$)
  - Now $1 + 2 + ... k + (k+1) = k(k+1)/2 + (k+1) = (k(k+1) + 2(k+1))/2 = (k+1)(k+2)/2$
  - Hence Proved.

Proof by Counter Example

- Consider a statement of the form
  - $\forall$ x $\in$ M, if P(x) then Q(x)
- Suppose that we wish to prove that this statement is false
- In order to disprove this statement, we have to find a value of x in M for which P(x) is true and Q(x) is false
- Such an x is called a counterexample
- Furthermore, proving that this statement is false is equivalent to showing that its negation is true
- The negation of the above statement is
  - $\exists$ x in M such that P(x) and not Q(x)
- Finding an x that makes the above statement true will disprove the original statement

Proof by Counter Example

- **Theorem** : Prove or disprove the statement that all prime numbers are odd.
- At first thought, it might seem that all prime numbers are odd.
- This is because it seems that all even numbers are not prime as 2 is a factor.
- However, by definition, 2 is a prime number but it is not odd.
- so we have found an example of when the statement is not true.
- This disproves the statement by counterexample.