Lecture 8: Proof techniques

Mathematical system: A system consists of Axioms, Definitions, and Terms is called a Mathematical system. We prove or disprove any statement within a mathematical system. Let us define some terms which are related to a mathematical system directly or indirectly.

1. **Definition:** A precise description or meaning of a mathematical term.
2. **Theorem:** A proposition that has been proved to be true. A theorem is of two kinds: Lemma and Corollary.
3. **Lemma:** A theorem that is usually not too interesting in its own right but is useful in proving another theorem.
4. **Corollary:** A theorem that follows immediately from another theorem.
5. **Conjecture:** A statement that is suspected to be true but yet to prove.

   Example: The 4-color conjecture, the $3x+1$ conjecture, Goldbach's conjecture, Hadwiger conjecture, the abc conjecture, etc.
6. **Axiom:** A statement that is assumed to be true without proof.

   Example: 2+2=4.
7. **Paradox:** A statement that can be shown, using a given set of axioms and definitions, to be both true and false at the same time.

   Example: Nobody goes to Murphy's Bar anymore as it's too crowded.

1 Methods of Proof:

By a proof, of a proposition $p \Rightarrow q$, we mean an argument that establishes the truth value of the proposition. Since the argument can be given in different forms and hence we can have different proof techniques.

1. **Direct Method:** Using p is true and with the help of other axioms, definitions and previously derived theorems, we here show that q is true.

   (a) **Example:** If m is odd and n is even integer, then show that $m+n$ is odd integer.

   Proof: We use the definitions of even and odd integer.

   m is odd if there is an integer k_1 such that $m = 2k_1 + 1$ and n is even integer if there is an integer k_2 such that $n = 2k_2$.

   Then $m+n = 2k_1 + 1 + 2k_2 = 2(k_1 + k_2) + 1 = 2k + 1$, where $k = k_1 + k_2$. So, $m+n$ is odd.

2. **Proof by Contradiction** In this technique, we assume that q is false, that is, $\neg q$ is true. Note that $\neg(p \to q) \equiv (p \wedge \neg q)$, that is to say, $p \to q$ is true if and only if $(p \wedge \neg q)$ is false. In other words, $p \wedge \neg q$ is a contradiction.

   (a) **Example:** For any integer x if x^2 is even, then x is even.

   Proof: Suppose x is not even and x^2 is even. So $x = 2k_1 + 1$ and $x^2 = 2k_2$ for some integers k_1, k_2. Then we have $(2k_1 + 1)^2 = 2k_2$. This implies $4(k_1^2 + k_1) + 1 = 2k_2$. But $4(k_1^2 + k_1) + 1$ is odd and $2k_2$ is even, so these cannot be equal. Thus we have a contradiction.

   (b) **Example:** Prove that $\sqrt{2}$ is irrational.

   Proof: Suppose $\sqrt{2}$ is rational. Then we can write $\frac{p}{q} = \sqrt{2}$, where $(p, q) = 1$.

   Then squaring both sides, we get $p^2 = 2q^2$. This implies p is even, that is, $p = 2k$ for some integer k. But then $q^2 = 2k^2$, that is, q is even. This gives a contradiction that $(p, q) = 1$.

   (c) **Example:** Prove that primes are infinite.

   Proof: Suppose there are only k primes $p_1, p_2, \ldots, p_k$. Now consider $n = p_1p_2 \ldots p_k + 1$. Since n is not a prime so there is some prime p_i such that p_i divides n. Also p_i divides $p_1p_2 \ldots p_k$. This implies p_i divides $n - p_1p_2 \ldots p_k = 1$. This is a contradiction as the smallest prime is 2.

   (d) **Example:** Prove that there are no integers x and y such that $x^2 = 4y + 2$.

   Proof: Suppose there are integers x and y such that $x^2 = 4y + 2 = 2(2y + 1)$. So x^2 is even and therefore x is even. Let $x = 2k$ for some integer k. Then substituting this, we get $2k^2 = 2y + 1$. But $2k^2$ is even while $2y + 1$ is odd, so these cannot be equal. Thus we have a contradiction.

3. **Proof by Contrapositive:** Note that $p \Rightarrow q \equiv \neg(p \wedge \neg q) \equiv \neg(\neg q \wedge p) \equiv \neg((\neg q) \wedge \neg(\neg p)) \equiv (\neg q \Rightarrow \neg p)$.

   Thus $p \Rightarrow q$ is logically equivalent to $\neg q \Rightarrow \neg p$. In other words, saying that if p is true then q is true is equivalent to if q is false then p is false.

   (a) **Example:** For any integer x if x^2 is even, then x is even.

   Proof: Suppose x is not even. So $x = 2k_1 + 1$ for some integer k_1. Then we have $x^2 = (2k_1 + 1)^2 = 4(k_1^2 + k_1) + 1$. This shows that x^2 is not even.

   (b) **Example:** Let a and b be integers. If $a + b$ is even, then a and b are either both odd or both even.

   Proof: Suppose that a and b are not both odd and both even. So one of a and b is odd and other is even. Without loss of generality, assume that a is even and b is odd. So $a = 2k$ and $b = 2l + 1$ for some integers k, l. Therefore $a + b = 2(k + l) + 1$. So $a + b$ is odd.

4. **Proof by Cases:** If $p \Rightarrow q$ and p is partitioned into cases r, s, that is, $p \equiv r \vee s$. Then from the below truth table, we see that $p \Rightarrow q \equiv (r \vee s) \Rightarrow q \equiv (r \Rightarrow q) \wedge (s \Rightarrow q)$.

r	s	q	$r \vee s$	$(r \vee s) \Rightarrow q$	$r \Rightarrow q$	$s \Rightarrow q$	$(r \Rightarrow q) \wedge (s \Rightarrow q)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	F	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

So if p as a proposition involves "or", it is sufficient to consider each of the possibilities for p separately.

(a) **Example:** Prove that there is no possible integer n such that $n^2 + n^3 = 100$.

Proof (Method 1): If $n^2 + n^3 = 100$ then we have

$n^2 \leq 100$ and $n^3 \leq 100$. This implies $n \leq 10$ and $n \leq 4$. So we have to check for the cases $n = 1, 2, 3, 4$. This gives the following cases:

For $n = 1$, $n^2 + n^3 = 1 + 1 = 2 \neq 100$,

For $n = 2$, $n^2 + n^3 = 4 + 8 = 12 \neq 100$,

For $n = 3$, $n^2 + n^3 = 9 + 27 = 36 \neq 100$,

For $n = 4$, $n^2 + n^3 = 16 + 64 = 80 \neq 100$.

Proof (Method 2): $n^2 + n^3 = 100$ is equivalent to $n^2(1 + n) = 100$. This is an expression of factors of 100 into two numbers n^2 and $1 + n$.

Note that possible divisors of 100 are : 2,4,5,10,25,50 and out of then for the possibility of $n^2 = 4$ and $n^2 = 25$.

Thus for $n^2 = 4$, $n = 2$ and $(1 + n) = 3$, then we get $n^2.(1 + n) = 4.3 = 12 \neq 100$,

Similarly, for $n^2 = 25$, $n = 5$ and $(1+n) = 6$, then we get $n^2.(1+n) = 25.6 = 150 \neq 100$.

(b) **Example** Prove that if n is an integer, then $n^2 \geq n$.

Proof: Proof is divided into three cases: (i) if $n = 0$ (ii) $n \geq 1$ is positive, (iii) $n \leq -1$ is negative.

Case 1: If $n = 0$, then $0^2 \geq 0$ holds.

Case 2: If $n \geq 1$, then multiplying both sides by n, we get $n^2 \geq n$.

Case 3: if $n \leq -1$, then since $n^2 \geq 0$, we get $n^2 \geq n$.

(c) **Example** Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers.

Proof: The proof is divided into four cases:

Case 1: When $x, y \geq 0$, the result holds.

Case 2: When $x \geq 0$ and $y < 0$, then $xy \leq 0$. So, $|xy| = -xy = x(-y) = |x||y|$.

Case 3: When $y \geq 0$ and $x < 0$, then as in Case 2.

Case 4: When $x < 0$ and $y < 0$, then $xy > 0$. So, $|xy| = xy = |x||y|$.

5. **Proof by Counterexample:** Suppose we have problem: Prove or disprove $A \Rightarrow B$. Thus if the proposition $A \Rightarrow B$ is not true then to show that $\neg(A \Rightarrow B)$ is true for some instances.

   If the problem is of the form $\forall\, x,\, A(x) \Rightarrow B(x)$, then its negation is $\exists\, x\, (\neg B(x) \wedge A(x))$.

   Thus to prove the original statement is not true, we have to find an x such that $(\neg B(x) \wedge A(x))$ is true.

   (a) **Example:** Prove or disprove: for all positive integetr n, $n^2 - n + 41$ is prime.

   Solution: Let us disprove by counterexample. If the statement is not true then we have to find a positive integer n such that $n^2 - n + 41$ is not a prime.

   Let $n = 41$. Then $n^2 - n + 41$ is equal to 1681, which is not a prime.

   (b) **Example:** Prove or disprove: for all positive inetegrs n, $2^n + 1$ is a prime.

   Solution: For $n = 1$, $2^n + 1 = 3$, which is prime.

   For $n = 2$, $2^n + 1 = 5$, which is prime.

   For $n = 3$, $2^n + 1 = 9$, which is not a prime.

6. **Existence Proofs:** An existence proof is a proof of a statement of the form $\exists\, x\, P(x)$. Such proofs are generally fall into one of the following two types:

   (a) **Constructive Proof:** Establish $P(x_0)$ for some x_0 in the domain of P.

   i. Example: Prove that If $f(x) = x^3 + x - 5$, then there exists a positive real number x_0 such that $f'(x_0) = 7$.

   Proof: Find $f'(x) = 7$, this gives $x_0 = \sqrt{2}$.

   (b) **Nonconstructive Proof:** Assume no x_0 exists that makes $P(x_0)$ true and derive a contradiction. In other words, use a proof by contradiction.

   i. **Example: Pigeonhole Principle**: If $n+1$ pigeons are distributed into n holes, then some hole must contain at least 2 of the pigeons.

   Proof: Assume $n + 1$ pigeons are distributed into n boxes. Suppose the boxes are labeled $B_1, B_2, \ldots, B_n$, and assume that no box contains more than 1 object. Let k_i denote the number of objects placed in B_i. Then $k_i \leq 1$ for $i = 1, \ldots, n$, and so $k_1 + k_2 + \ldots + k_n \leq 1 + 1 + \ldots + 1 \leq n$. But this contradicts the fact that $k_1 + k_2 + \ldots + k_n = n + 1$, the total number of objects we started with.

7. **Proof by Induction:** There are two form of mathematical induction. One is weak form and another is strong form. We discuss them separately.

   (a) **Weak Form of Mathematical Induction:** Let $P(n)$ be a statement on positive integer n such that

   1: $P(1)$ is true,

   2: for all $k \geq 1$, $P(k+1)$ is true whenever one assumes that $P(k)$ is true.

   Then $P(n)$ is true for all positive integer n.

   i. **Example:** Prove that $1+2+\ldots+n = \frac{n(n+1)}{2}$.

   Proof: Let $P(n) = 1+2+\ldots+n$. Then $P(n)$ holds for $n=1$.

   Suppose $P(n)$ holds for $n=k$, that is, $P(k) = 1+2+\ldots+k = \frac{k(k+1)}{2}$. Now we show that $P(n)$ is true for $n = k+1$.

   $P(k+1) = 1+2+\ldots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$. Thus $P(n)$ holds for every n.

   ii. **Exercise:** Prove that $1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6}$.

   iii. **Exercise:** Prove that for any positive integer n, $1+3+\ldots+(n-1) = n^2$.

   Corollary of weak form of mathematical induction: Let $P(n)$ be a statement on positive integer n such that for some fixed positive integer n_0

   1: $P(n_0)$ is true,

   2: for all $k \geq n_0$, $P(k+1)$ is true whenever one assume that $P(k)$ is true.

   Then $P(n)$ is true for all positive integer $n \geq n_0$.

   (b) **Strong Form of the Principle of Mathematical Induction:** Let $P(n)$ be a statement on positive integer n such that

   1: $P(1)$ is true,

   2: $P(k+1)$ is true whenever one assumes that $P(m)$ is true, for all m, $1 \leq m \leq k$.

   Then $P(n)$ is true for all positive integer n.

   Corollary of strong form of mathematical induction: Let $P(n)$ be a statement on positive integer n such that for some fixed positive integer n_0,

   1: $P(n_0)$ is true,

   2: $P(k+1)$ is true whenever one assume that $P(m)$ is true, for all m, $n_0 \leq m \leq k$.

   Then $P(n)$ is true for all positive integer $n \geq n_0$.